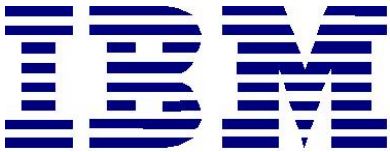
State of Missouri
Strategic
e-government Architecture

A Plan for
Missouri's e-government Architecture



IBM Global Services
1005 Ikon Drive, Suite G
Jefferson City, MO 65109

October 1, 2000

Part One – Project Summary

International Business Machines Corporation (IBM), the State of Missouri Chief Information Officer and the e-government committee of the Information Technology Advisory Board (ITAB) collaboratively developed the State of Missouri's Strategic e-government Architecture. IBM's e-business strategic methodology was employed to gather and analyze information. IBM intellectual capital assets were used to identify and apply best practices.

The focus of the present e-government strategic analysis is on architecture. Other topics, including process and organizational aspects, are beyond the scope of the present analysis.

1 Document Overview

When considering the target audience for this project's Final Report, it was recognized there are at least five principle audiences:

- Information Technology Advisory Board (ITAB)
- ITAB e-government subcommittee
- Chief Information Officer, State of Missouri
- IT Architecture Working Group
- State Executives, Elected Officials and the Legislature

In recognition of these distinctions and their particular information needs, the Final Report has been broken into four parts, with a consolidated Appendix.

- Part One – Project Summary (current document) outlines the project approach and activities implemented to gather information.
- Part Two - Executive Summary contains the Executive Overview, Recommended Architectural Summary, and recommended next steps.
- Part Three – Findings, contains the observations from the Executive and Technical Interviews. It provides a brief description of the e-government vision, architecture, and technical initiatives.
- Part Four – Reference Architecture, contains recommendations for the development of an e-government framework

2 The Process

The State of Missouri's e-government must be more than a collection of technologies and products. It will require the combination of several architectural styles, much like a city plan. Figure 1depicts these architectural styles. The focus of this analysis is on the operational (infrastructure) architecture. Concurrent with this analysis, the State of Missouri is analyzing the functional (business processes) architecture. The other architectural areas are important and will need to be considered and addressed as the State of Missouri moves forward.

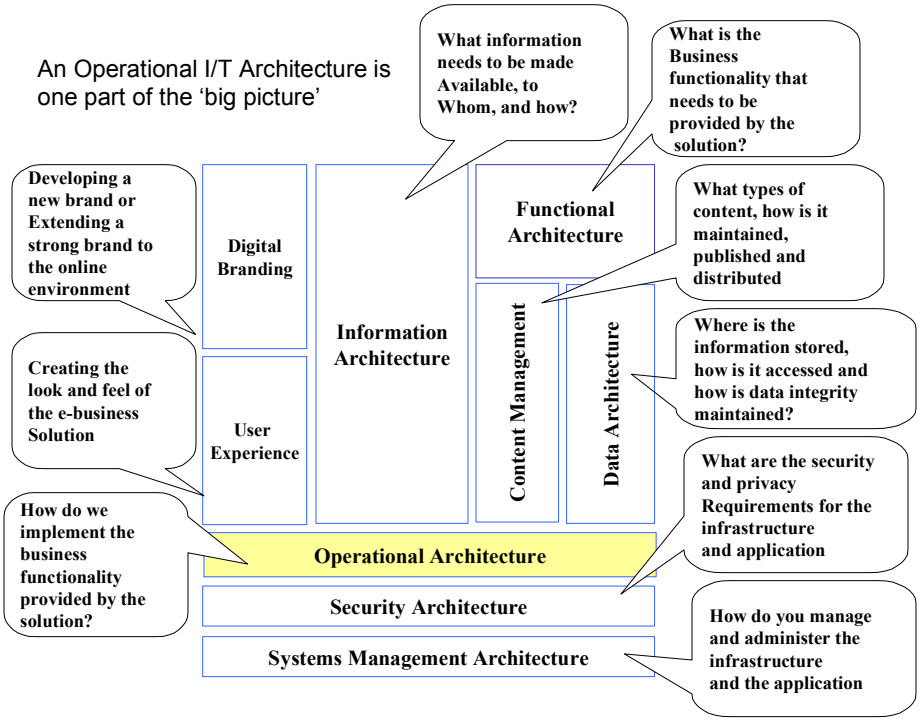


Figure 1, Architectures

This project included the development of an e-government technology architecture and the development of a demonstration portal. Development of the e-government technology architecture was done using a seven-step study process. The objective of the first three steps was to document the business drivers, strategies, and architectures. This information was gathered through interviews and from existing best practice documentation and is the foundation used to develop the technology architecture.

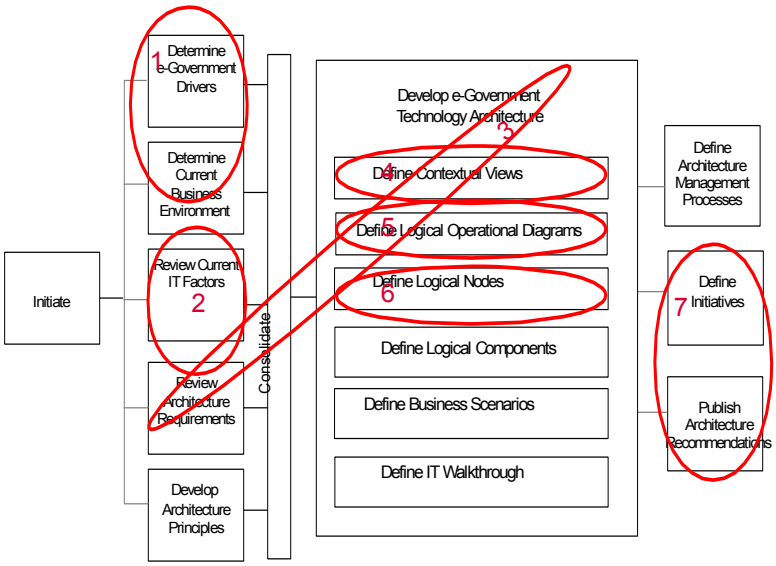


Figure 2, Project Approach

The seven-step process, depicted in Figure 2, Project Approach, consisted of the following steps:

1. Document business drivers and strategy (Executive Interviews)
2. Document current I/T environment, the application models, infrastructure and technologies (Technical Interviews)
3. Identification of significant current solution patterns (Workshops)
4. Establish an application reference architecture
5. Establish a technical reference architecture
6. Define I/T services (logical nodes)
7. Delivery of an e-government Architecture Plan report and presentation to Missouri state government IT management

2.1 Document business drivers and strategies

Documenting the business drivers and strategies is essential to establishing well-grounded technical architecture. The real value of a technical architecture is to build a robust infrastructure to support the changing requirements of the business.

The Missouri Chief Information Officer and IBM conducted twenty-six interviews with Department and Office Executives/Directors and other representatives of the executive and judicial branches. (Refer to Appendix for the list of Executive Interview Participants.) These interviews were intentionally left open-ended so that the executives would respond in the context of their responsibilities and not limit their answers to preconceived notion. Each interviewee was asked:

- What is your domain of responsibility?
- What issues and challenges do you face?
- How do you anticipate the business changing in your area of responsibility?
- What would enable you to reach your goals more effectively/easily?

From IBM, Karl Staub, IBM I/T Architect, and either Bob Dill, IBM e-business Architect, or Mark Clement, IBM I/T Architect attended each interview. Major points were summarized during each interview to ensure they were understood. The interview closed with two final questions:

- Were there any other issues of which we should be aware?
- Would the interviewee please contact Karl Staub with any further developments or information, which might arise, that should be considered?

After the interviews, the raw interview notes were transcribed into a database for future reference, and synthesized by the team. In addition the State of Missouri provided a large volume of documentation for review. (See Appendix for a list of documentation received.)

2.2 Document current I/T environment

Under the guidance of Deputy CIO, Larry Seneker, key information systems were selected for review. These systems were selected to represent the wide scope of platforms, application models, programming languages, dependencies, and functions. From these reviews we created a high level view of the current IT infrastructure.

2.3 Joint Workshops

A number of joint meetings between the ITAB e-government subcommittee, the Office of Information Technology and the IBM Project team occurred throughout the project. These workshops included:

Kickoff Session

The project was launched with a joint kickoff meeting where the IBM project team was introduced to the ITAB e-government subcommittee. A general discussion of the project activities and timeline was conducted as well as an introduction to the e-government architecture.

Joint Working Sessions

The results of the executive and technical interviews were then presented to the e-government subcommittee of the ITAB in a half-day session conducted at the IBM facilities. These findings were then augmented and enhanced through discussions with the subcommittee and are the basis for the findings presented in this report.

The second day session continued the discussions of the business findings and the development of the initiatives required to implement the Missouri's e-government architecture.

Instructional Sessions

Two instructional sessions where added to the scope of this project to introduce the concepts of an enterprise architecture in general and the reference architecture for e-government in detail. The original target audience was the e-government subcommittee. We extended the offering, through a second session, targeting IT Directors and IT Architects. This was an open invitation for any interested party within the state. This invitation was distributed via Larry Seneker.

Electronic copies of the presentation were delivered to the Office of Information Technology. They are also included in this deliverable as Attachment 1.

2.4 Establish an Application Reference Architecture

A single application reference architecture is favored by most organizations -- not as the sole model for all future application development, but as a conceptual reference point for application modeling. The benefit of a reference application architecture is that it:

- Enables application packages to be evaluated for business functionality, as well as the ability to be integrated into the existing infrastructure.

- Provides a consistent means to estimate the effort and cost for anticipated systems integration requirements of a particular application
- Provides a way for development technologies to be selected while creating applications, which can interoperate on an evolutionary basis.

There are a variety of application architectures, which may be applicable and effective for Missouri State Government. The business drivers, goals, and issues identified in the first step of this assessment process are used to identify which general application model would be most effective. This will impact, and be impacted by, the development process and methodology currently in place.

A mismatch between application architecture and application development methodology results in slower development and deployment. More often, it results in wasted capital as inflexible applications are developed and deployed.

2.5 Establish a Technical Reference Architecture

A technical reference architecture is a type of reference architecture that does not directly include structures of application (business) behavior[1]. In other words, it can be used as a base architecture or template for several different application types.

In our definition, a reference architecture includes both functional and operational aspects of an IT system. The functional aspect is concerned with the functionality of collaborating software components; the operational aspect is concerned with the distribution of components in order to achieve the required service level characteristics. A reference architecture is not only a software architecture; it also provides predefined structures for the placement of software on hardware nodes, and structures for hardware connectivity.

The technical reference architecture supports and constrains the application reference architecture. The application (business and industry specific) part of the architecture uses the structures provided by the technical reference architecture.

The technical reference architecture is effective only when viewed as part of the entire IT environment. The entire IT environment is comprised of the application and technical reference architectures, organizational principles and policies, business processes, culture, and environmental forces. Architecture documents at Missouri State Government include most of these items.

---

[1] Intellectual capital assets from IBM's Enterprise Solutions Structure (ESS) were used to develop this technical architecture. ESS provides a standard architectural framework to support creation, reuse, and maintenance of architecture and design assets. ESS draws on experiences with building customer solutions to distill "best practice" structures, models, and sample deliverables.

In this step of the process, the technical reference architecture is defined as "***the technical blueprint for evolving a corporate infrastructure resource that can be shared by many users and services.***"[2] To achieve this objective, other factors (e.g., organization, processes, etc.) are intentionally separated from the definition of the technical reference architecture. (This does not imply that these other factors are unimportant. It is essential they be addressed in an overall plan to deploy applications rapidly to support the business.)

2.6 Define I/T Services (Logical Nodes)

Based on the technical reference architecture and the essential business and technology drivers, the next step is to identify the logical nodes required to support the current and projected requirements.

Logical nodes illustrate the interaction between users, applications, and data. They identify essentially three things:

- The services they deliver
- The nodes on which they depend
- The standards which define them

2.7 Delivery of A Plan for Missouri's e-government Architecture

A Plan for Missouri's e-government Architecture reviews the assessment process, the existing I/T environment, and the conclusions drawn from the analysis of the information. This includes specific recommendations for the application and technical reference architectures as well as recommendations in other areas where significant issues have been identified. It is intended to help launch the reference architecture as an ongoing, vital process for Missouri State Government.

2.8 Deliver a Portal Proof of Concept

The key mechanism to developing a common view of state government is the creation of a portal or common interface for accessing state government services and information. This project will deliver a prototype of a state portal and is intended to demonstrate the portal concept. The user interface represents two possible layout and navigation options

[2] Every Manager's Guide to Information Technology, Peter G.W. Keen, Harvard Business School Press, Boston, 1991, p.32

and clearly demonstrates the value of a "common look and feel", and "one door" access to Missouri information and services.

3 General Observations

A primary purpose of this project was to determine what, if any, common components of Missouri's e-government infrastructure should be provided in a shared fashion. To determine the possible common components, Missouri's e-government reference architecture was developed. This reference architecture leverages the work that the state has done to establish an Enterprise Architecture.

The project considered the current organization of the executive departments and the supporting I/T systems and organizations. These were treated as constraints and not subject to review.

This project was initially limited to focus on the delivery of government services to citizens and businesses through the Internet. During the executive interviews it became apparent that employees of the state should also be considered. Several executives spoke of the need for employees to have access to comprehensive information spanning the organizational structure of Missouri state government. Additionally the need to deliver employee benefit information was identified.

The executives consistently spoke about the need to improve customer (generally citizens and businesses) service. They identified that the delivery of services should be by program (i.e. workforce investment act) as opposed to the department / division / agency structure.

This business vision of integrated services, will require the integration across organizational boundaries. To support integration there is a need for standards and common architectures.

One of the major catalysts for the rapid growth of the Internet is the adoption of standards by the industry. These standards allow for interoperability but will not, in and of themselves, address the need for application integration. The standards do form a basis that make it possible to build independent heterogeneous I/T systems that **can, with appropriate design,** work together.

The diverse I/T organizations that exist within the state are not likely to fully adopt one statewide application architecture. Therefore, it is important that the State of Missouri adopt a common statewide application integration architecture.

The environment of the State of Missouri calls for the implementation of "hub and spoke" application integration architecture. The spokes are the individual I/T systems supporting departmental program implementation. The hub provides the mechanism to compose an integrated, single interface to those independent systems.

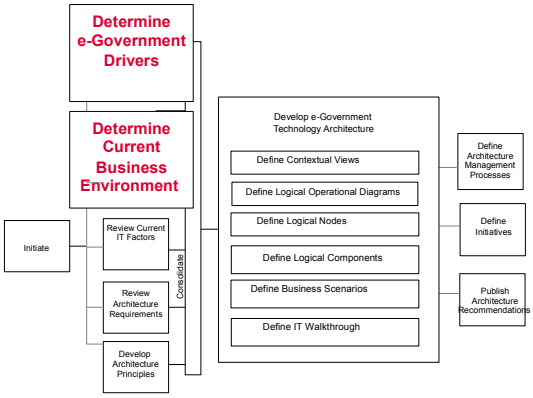
While the State of Missouri is well positioned to begin to implement electronic delivery of government services, there are several significant gaps:

- Adoption of Internet / intranet technologies is likely to have a significant impact on the I/T infrastructure.
    - Server, storage and network capacity increases will be needed. The growth in network capacity is of concern given the number of locations that the state supports.
    - Resources to support e-commerce (for example, credit card processing) are not yet in place. New resources and services will need to be procured.
- I/T skills needed to implement e-government are not widely available within the state.
- Executive involvement was apparent during the project. Executive leadership is key to the successful transformation of service delivery. There is a need to establish an ongoing process to communicate both the value and the challenges that exist within this endeavor to the executives.
    - Issues that impact multiple I/T departments will become more common (for example, should a common user navigation and brand image be conveyed, or should it be at a departmental level and what services should be provided through shared resources?). Appropriate resolution will require informed executive leadership.
- The State of Missouri's work developing an Enterprise Architecture needs to continue.
    - The state will need to expand and elaborate on its architectural guiding principles. These principles should serve as a common basis for consideration of detailed architectural issues.
    - The state will need to define and implement an Architectural Management Framework. That framework must define the necessary processes, roles and responsibilities in order to ensure the orderly on-going development and evolution of the state e-government I/T Architecture.
    - The state will need to determine an application integration architecture.
    - The state should address and plan for systems management.
- Significant security issues need to be addressed. The common components will need to be secured from both external and internal threats. User authentication supporting access to multiple departmental systems will need to be provided.

Part Two - Executive Summary

The State of Missouri wants to better serve its constituents by providing information and services via transactions over the World Wide Web. This use of e-business technologies to deliver government services is known as e-government. There are a number of topics that will need to be addressed as the State of Missouri moves forward with e-government implementation. The focus of the present e-government strategic analysis is on architecture. Other topics, including process and organizational aspects, are beyond the scope of the present analysis. The primary focus of this architecture is on core services and common infrastructure components.

Successful e-government architecture must be aligned with the business of the State of Missouri. As shown in the figure to the left, both the current business environment and the e-government drivers served as input during the development of this plan. Key input came from interviews of elected officials, department directors, the Missouri Supreme Court, and a number of directors of other state agencies. This input is reflected in the design decisions, standards, interfaces, and common services.



The analysis found a number of common themes or, drivers, of Missouri's e-government architecture that are listed below.

Improve Delivery of Services to Citizens and Business

Citizens and businesses operating in Missouri should be able to access a number of basic government services via the Web. These services should be delivered through a single convenient point of access. This single window, or portal, should deliver services that are integrated and cross the current organizational structure. An individual should not be required to understand the organizational structure of this government in order to locate information and/or services.

There is a great opportunity to improve service delivery through increased accessibility. The executives indicated that requiring a constituent to visit the appropriate agency during normal business hours would not be acceptable in the near future. Constituents should be able to interact and perform the business of government when and where they want. Barriers of time and distance must be removed. Today this is popularly referred to as "moving from in-line to on-line."

A major issue that the executives indicated needed to be considered is the "digital divide". While more Americans than ever have access to the Web, there are people who

for one reason or another don't have access to the Web. The difference between these two groups of people is what is referred to as the "digital divide". The benefits of e-government services should, as far as possible, be available to everyone. E-government services should be available through public Internet access sites, such as public libraries. As the technologies mature new and different interfaces to e-government should be provided, these might be wireless phones, personal digital assistants, low cost network appliances, kiosks, Web TV, telephone call centers, and so on. It means that state employees who work with the "digitally disadvantaged" need immediate access to the same services as Missouri citizens have.

Increase Cost Efficiencies

Several factors drive a desire to improve cost efficiencies within the State of Missouri. Delays and lag time due to bureaucracy should be reduced. Constituents should be provided with self-service capabilities where appropriate. These require new and unique ways to deliver government services.

Invest in Partnerships

Partnerships with private sector and / or other public agencies are becoming increasingly important. This drives a need to both gather information from partners and provide information to partners. The use of industry standard technology that allows interchange of information between partners is necessary.

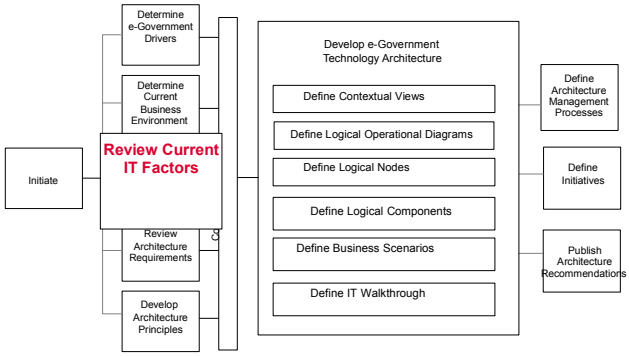
Drive Economic Development

One of the priorities of the State of Missouri is economic development. Integration and cooperation within and between the departments of government should be improved to reduce redundant paperwork and the resultant costs of compliance on business. This and other actions should help to reduce inappropriate burdens due to inefficiencies within government and make Missouri more business friendly.

1 Current Environment

The greatest proportion of state services are delivered through the sixteen departments within the executive branch of the State of Missouri. These sixteen departments, and the divisions, bureaus, sections or units that comprise them, operate independently and have distinct missions. At times these mission range from overlap through separation to conflict. These departments interact with businesses and / or with one another, at times dealing with the same constituent. This compounds the complexity perceived by citizens and businesses interacting with state government.

2 I/T Environment



Another key requirement for Missouri's e-government architecture is to ensure that takes into consideration the current I/T environment within the State of Missouri. The current I/T environment in conjunction with industry-wide I/T experience and trends guided the development of this e-government architecture plan. This architecture, and the Enterprise Architecture that it is a part of, are adaptive architectures that where appropriate will leverage the existing I/T investments within the State of Missouri. This will allow an effective transition to the new architecture.

As with any organization the size of the State of Missouri, there is an extensive portfolio of I/T systems supporting its business functions. Those systems represent a considerable number of application models and operational environments.

A simplified illustration of the current I/T environment is presented in the figure, Business and Technology Isolation. Each of these boundaries represents additional complexity that must be bridged in order to fully implement e-government.

Each of the departments represents an organizational boundary. To simplify the chart a limited number of agencies are represented, and no external organization is included. Also, many departments are comprised of independent business units that create additional organizational boundaries.

The technology silos represent distinct technology platforms that exist within each of the selected departments. Four widely deployed operating environments are depicted. Within each platform there are differing application styles that create additional boundaries that for simplicity are not included.

This simplified figure illustrates that a large number of boundaries exist. This architecture is intended to reduce the proliferation of unique technology platforms and to enable the integration across boundaries.

3 Comprehensive Vision.

There are hundreds of potential transactions to enable electronic delivery of a vast number of government services. These services must be delivered in an integrated manner that reduces complexity. Reducing complexity for citizens and businesses will be accomplished by providing an integrated point of comprehensive, ubiquitous, and useful access to government services, information (data), and people. The adoption of a consistent architecture for the delivery of e-government services will reduce the complexity for the state.

4 Architecture

Missouri's e-government architecture is intended to guide the implementation high-function Web applications using open, vendor-neutral standards. The architecture is based on an n-tier distributed environment. In its most basic form, the architecture can be depicted as a three-tier model. Tiers of presentation, application logic and business services are separated into components, and connected via industry-standard protocols, servers, and software connectors. It is important to note that this architecture incorporates integration services. This tier will serve as the hub in a hub and spoke relationship with the underlying operational I/T systems that exist within and support the departments.

This architecture supports the integrated single window, or portal, into the State of Missouri. It supports the implementation of Web based transactions to enable specific government services. It leverages the existing I/T investments of the State of Missouri. It leverages future I/T investments by providing both common e-business application architecture and by supporting common operational infrastructure.

5 Gap Analysis

Gaps exist that must be addressed if the State of Missouri is to maximize the benefits from its expenditures on e-government projects. These gaps relate to the:

- The State of Missouri needs to continue to develop Enterprise Architecture for I/T.
- There needs to be a consistent model for integration of applications.
- Current I/T infrastructure including server, storage, and network capacity within specific departments will need to be enhanced to facilitate the delivery of e-government services both to external constituents and within the departments.
- I/T skills needed to implement e-government will need to be expanded within the state.
- Policies and procedures that establish the legal framework for e-government need to be elaborated.

6 Next Steps

This project focused analysis on the architecture needed for the technology to deliver e-government. There are significant issues, not related to this architecture, that need to be addressed. These are likely to require senior executive decisions. For example;

- Funding priorities for implementation of specific government services.

- To what degree will a common look and navigation model will be adopted (and enforced).
- Which, if any, executive departments have independent brands.

Six technology initiatives were determined to be appropriate during the joint IBM / State of Missouri workshop. They are:

1. Implement an Interagency Zone to protect common e-government resources from inappropriate intrusion.
2. Embrace a Portal Framework that provides a single point of access for data, applications and processes and deliver personalized views of information and processes where users search, integrate and manage a wide variety of data and processes
3. Adopt Common User Authentication in which a user logs on once to gain access to all portal resources and, if appropriate, supports digital signatures to authenticate the source.
4. Implement a Credit Card / Payment Gateway to support the use of credit card by citizens and businesses.
5. Adopt an Enterprise Application Integration architecture that provides simplified access to the disparate departmental I/T applications.
6. Define Common Commerce Services to allow agencies to offer goods or services through the Internet.

7 Conclusion

The State of Missouri executives were engaged and excited about the potential of e-government. They consistently spoke about the need to improve customer service, reduce costs, and create a more effective state workforce. These objectives translate into integration across organizational boundaries. To support integration there is a need for standards and common architectures.

One of the major catalysts for the rapid growth of the Internet is the adoption of standards by the industry. These standards allow for interoperability, but an appropriate architecture is needed to facilitate the necessary application integration. The diverse I/T organizations within the state are not likely to fully adopt a single statewide application architecture. The State of Missouri should focus on the adoption of common application integration and operational architectures.

The State of Missouri should adopt a roadmap to become an e-government. One of the key messages that is consistent from the consultant community is that the adoption of e-government (or e-business) is not a single I/T project, but an ongoing series of actions that are repeated for each successive e-government enhancement. Dramatic improvements in both service and cost efficiencies will be realized when business

processes are transformed using Internet technologies. Successful delivery of e-government services will be achieved through starting simple and growing fast.

Part Three - Findings

1 Overview

The State of Missouri wants to use e-business technologies to better serve its citizens and businesses. This government of the future is referred to as an e-government. The most common characteristic of e-government is the provision of online services (or transactions) and information through the Internet. This document addresses important considerations for the State of Missouri as it embarks upon becoming an e-government.

2 Drivers of e-government

This section describes the findings from the analysis completed. Listed below are the main strategic business results that the State of Missouri has indicated they want to achieve through the use of e-business technologies.

- Improve Delivery of Services to Citizens and Business
- Increase Cost Efficiencies
- Invest in Partnerships
- Drive Economic Development

2.1 Improve Delivery of Services to Citizens and Business

The State of Missouri is driven by both internal and external forces to improve the quality of and access to government services. Missouri's government improvement programs and legislation create internal "push". External "pull" is driven by the increasing demands from constituents to go online. These drivers can be separated into three fundamental categories:

- Reducing Government Complexity
- Simplifying Government Interactions
- Improving Access

2.1.1 Reducing Government Complexity

The need to reduce the complexity of interfacing with Missouri government has been recognized. The **Official Manual of the State of Missouri for 1999-2000** states:

> *'a broad network of government organizations has been created to accomplish the purpose. Because of the many different names used by these groups—departments, divisions, agencies, boards, commissions, bureaus, units, sections, programs and others—it can be difficult to determine which area of government is responsible for certain services, or to sort out responsibilities or relationships within the governmental framework.'*

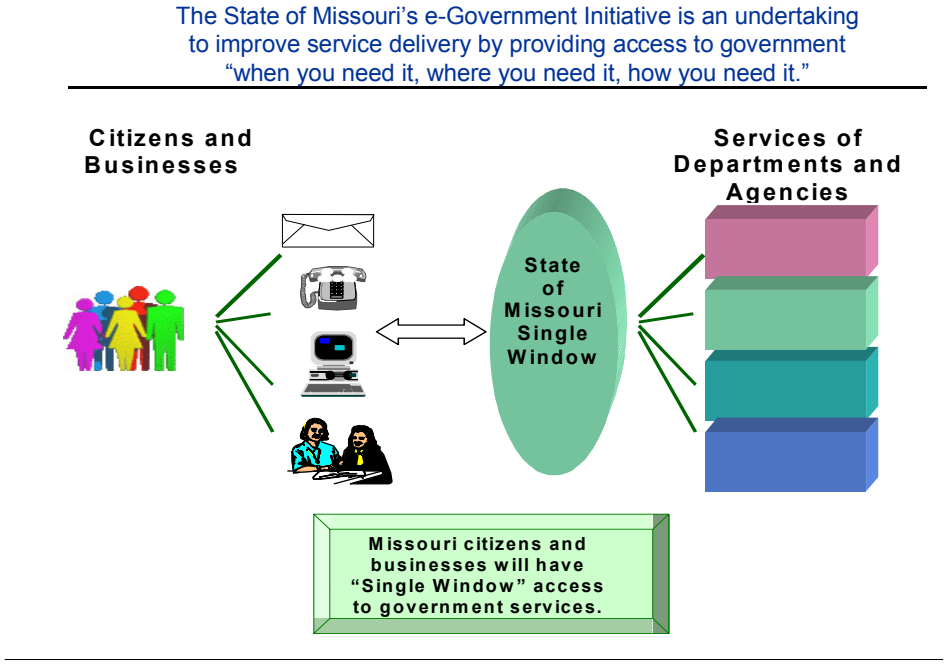


Figure 3

As depicted in Figure 3, constituents should be shielded from the complexities inherent in the structure of the State of Missouri. A principal desire is to provide citizens and businesses with a single window, or portal, into the government services. A citizen should not have to understand the organizational structure of government in order to locate information and/or services provided by government.

This will require integrated services. These integrated services are organized by program (i.e. workforce development) rather than by often confusing organizational structures. The delivery of integrated services will require "virtual agencies". A "virtual agency" combines several governmental entities (state and other levels) to provide information and services in a seamless manner. Often private entities are involved with delivery of the program. The State of Missouri has several examples in this area, among them:

- The Workforce Development System, driven by the Workforce Investment Act, integrates employment and training services into "One-Stop" sites. The Departments of Economic Development, Labor and Industrial Relations, Social Services,

Elementary and Secondary Education, and Higher Education have partnered to provide Missourians employment and training services through the One-Stop system.
- The Caring Communities Initiative, developed to form a more productive relationship between state agencies and local jurisdictions, spans the Departments of Labor and Industrial Relations, Elementary and Secondary Education, Social Services, Health and Mental Health, Economic Development and Corrections.

2.1.2 Simplify Government Interaction

Another desire that was common through the project is the need to simplify the State of Missouri's interactions with its constituents. Current examples within the State range from:
- Elimination of requirements to register or report.
- Reductions in complexity for registration or reporting.
- The consolidated application for discretionary grants for school districts reduces the need to complete multiple applications, eliminating redundant work.
- SCR 29 - Relating to streamlining and simplifying sales and use tax imposition and collection.

2.1.3 Improved Accessibility

Perhaps the greatest opportunity to improve service delivery is through increased accessibility. The State of Missouri indicated that the existing model of interaction that requires a constituent to visit the appropriate agency during normal business hours would not be acceptable in the near future. Overcoming the barriers of time and distance to perform the business of government and give people public information and services when and where they want it is the basis of becoming an e-government.
The State of Missouri cannot choose its customers. It must make certain that, as far as possible, the benefits of e-government are available to everyone. The adoption of Internet technology has been fast and widespread. Some constituents have not been as fast to adopt the technology. The disadvantaged need to be served just as much as the more affluent, capable and connected sections of society.
Access to some e-government services will need to be provided in different languages, and for users with differing abilities. Finally, Missouri must deal with and serve users across a large spectrum of sophistication and familiarity with technology: from complete beginners, including "net-phobics", through to I/T-literate large businesses.
The State of Missouri's must eventually enable as many different interfaces to e-government services as possible. Accessing e-government services might need to be via handheld devices, low cost network appliances, kiosks, Web TV, Playstations, telephone call centers, and so on.

2.2 Increase Cost Efficiencies

Both internal and external forces drive the State of Missouri. Missouri's government improvement programs are internal "push". The external "pull" is the shifting of

responsibilities from federal to state levels and the increasing demand for efficiency, effectiveness, and accountability from taxpayers.

2.3 Invest in Partnerships

Partnerships with private sector and / or other public agencies are becoming increasingly important. In this case there are a number of forces providing the internal "push". They primarily relate to the need to use external resources to meet the goals of specific programs. External "pull" is provided by the need for comprehensive information about partnerships. This information includes reliable and complete cost data. It also includes the need for enhanced monitoring and oversight to evaluate compliance and performance. The State of Missouri has increased the use of various types of cooperative partnerships over the past several years. A Council of State Governments' survey found that state agencies responsible for social services, transportation, mental health care, corrections, health, and education had all increased partnerships (or privatization) activities and found a trend toward expansion of this across major state agencies.
A very abbreviated list of partnerships within the State of Missouri includes:

- The Workforce Development System combines state departments, local public agencies, community organizations, and the private sector.
- The Caring Communities Initiative was developed to form a more productive relationship between state agencies and local jurisdictions.
- The Department of Economic Development uses public/private partnerships to build economic opportunities.
- The Department of Social Services counts on "partnerships with local communities and other state agencies to achieve the best outcomes for Missouri's most vulnerable citizens."
- The Missouri Transportation Research and Education Center is a partnership between University of Missouri and the Missouri Department of Transportation.
- Water Quality coordination includes the departments of Agriculture, Natural Resources, Conservation, Health along with other public and private entities.
- The Rural Economic Assistance Program (REAP) involves the Departments of Agriculture, Economic Development, the University of Missouri, and others.
- The Missouri Market Development Program includes the Departments of Economic Development and Natural Resources along with the University of Missouri Outreach and Extension and Missouri Enterprise/MAMTC.

2.4 Drive Economic Development

An increasing priority for the State of Missouri is the ability to drive economic development up. The internal "push" is the focus on increasing the economic well being

of Missourians. External "pull" includes competitive pressures from other jurisdictions and the increasing demands from constituents.
There are many activities to drive economic development within the State of Missouri, examples include:

- The Agri Missouri market development program within the Department of Agriculture.
- The development of Missouri's workforce through the efforts of the Departments of Economic Development, Labor and Industrial Relations, Social Services, Elementary and Secondary Education, and Higher Education.
- The Department of Economic Development activities to create economic opportunities.
- The Department of Insurance works to maintain consistency with other states to minimize the costs to industry.

There is clear evidence that governments can increase economic development through investments in I/T. Robert L. Mallett, Acting Secretary United States Department of Commerce, at the E-Gov 2000 Conference, stated "After the ballot box, I cannot think of a greater, more powerful tool for advancing democratic rights and economic opportunity than the Internet and eGovernment."

3 Current Environment

3.1 Organization

The Missouri Constitution (Article II, Section 1) states: *"The powers of government shall be divided into three distinct departments—the legislative, executive and judicial." This section also prohibits persons within each branch from exercising powers of the other branches. From these three branches spring the variety of organizations which deliver services of state government. Generally speaking, the legislative and judicial branches rely on committees or other small, appointed groups to perform research, develop policy, provide advocacy services or handle administrative duties. In these two branches, most services are delivered through the offices of the elected officials themselves and not by related agencies.*
It is through the executive branch that the greatest proportion of state services are delivered. The Constitution (Article IV, Section 12) and the Reorganization Act of 1974 have established a number of "executive departments" to deal with specific areas of interest. The Missouri Constitution provides for 16 specific departments: the Office of Administration and the departments of Agriculture, Conservation, Corrections, Economic Development, Elementary and Secondary Education, Health, Higher Education, Insurance, Labor and Industrial Relations, Mental Health, Natural Resources, Public Safety, Revenue, Social Services and Transportation.
Within each executive department exist a variety of offices of varying size and scope which deal with specific services. Traditionally, "divisions" are the next-largest

organizations within departments and function to bring together smaller-sized groups, such as "bureaus," "sections" or "units."[3]

3.2 Department Interactions

During this project each of the department directors (or their designate), elected officials and several agency directors were interviewed. One of the objectives of this interview process was to identify the interactions that exist between departments and other state departments (or agencies), businesses, citizens, and government bodies. This is necessary input to understanding what will actually be required to do something as desirable as, for example, simplifying citizen interactions with the state. These diagrams are accurate representations of the interactions for each agency, but are not an exhaustive analysis for any single agency. Consider the following diagram, created after interviewing the Governor's office.

This diagram shows that the primary interactions from the Governor's office are everywhere. They link to the Federal government, other states, all the different state bodies, local businesses and citizens. Many of the individual diagrams approach the simplicity of this diagram to at least one of the groups identified here. In fact, if this were all that had to be addressed, the state would have to do very little to create a simple interface for all of its important constituents.

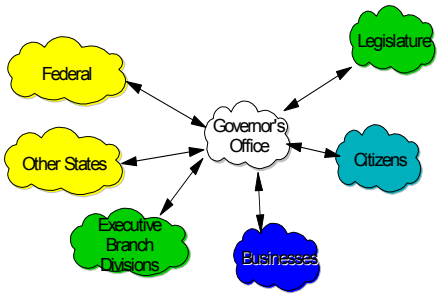


Figure 4 below illustrates the Department of Revenue relationships. It is not much more complex than the Governor's office, but it does begin to introduce the complexity present in any state government.

[3] The Official Manual of the State of Missouri for 1999-2000.

Figure 4

As patterns continue to be uncovered, other forms of organizational interaction appear. Here, the one-way relationship between DOLIR and a variety of state agencies, related businesses, and citizens appears. Specific state and Federal agencies are identified, and the fact that businesses and citizens have simultaneous relationships with other interested organizations becomes apparent.

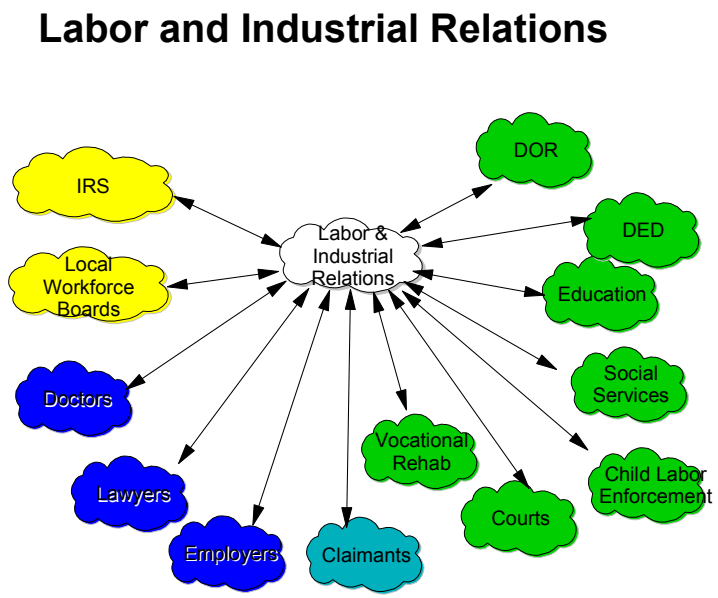
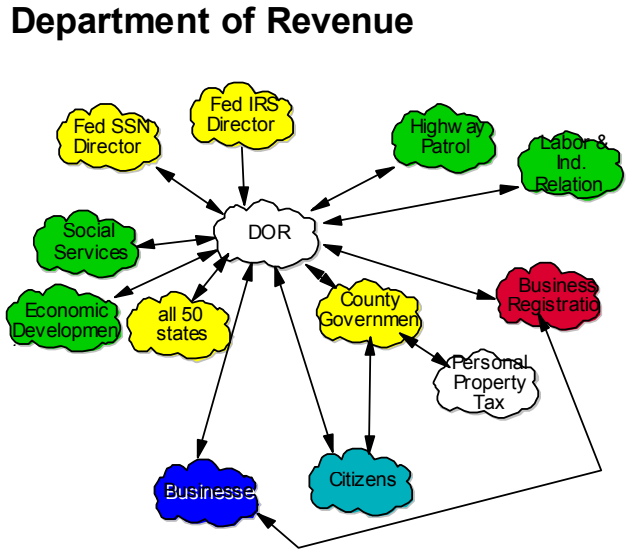
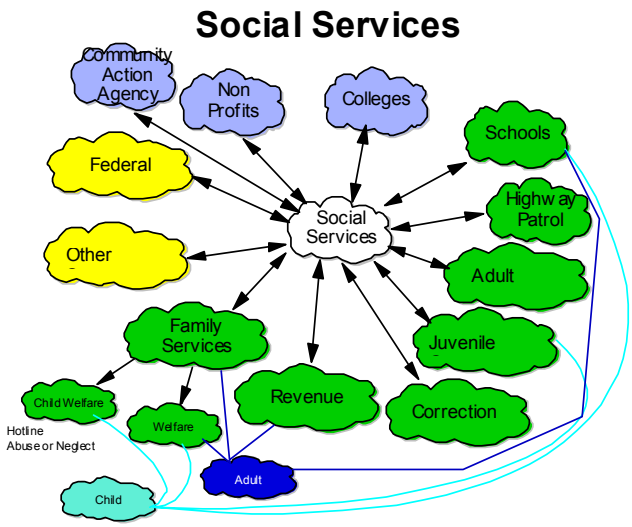


Figure 5



The last agency pattern to be presented here is from the Department of Social Services, which has the most complex interactions of any part of the state inspected here. Now a wide variety of interactions appear between social services and the breadth of services used by their clientele. This is not to indicate that every person who uses social services interacts with all the agencies as depicted in this diagram, but that this breadth of



interaction exists across the population Social Services serves.

Again, as for each of the preceding diagrams, it is not difficult to determine how to create a simplified interface to this single agency for a single group of users. The challenge is in addressing this issue for the enterprise of state government. Why this is the case becomes obvious when several of the preceding diagrams are combined into a single chart such as illustrated in Figure 6.

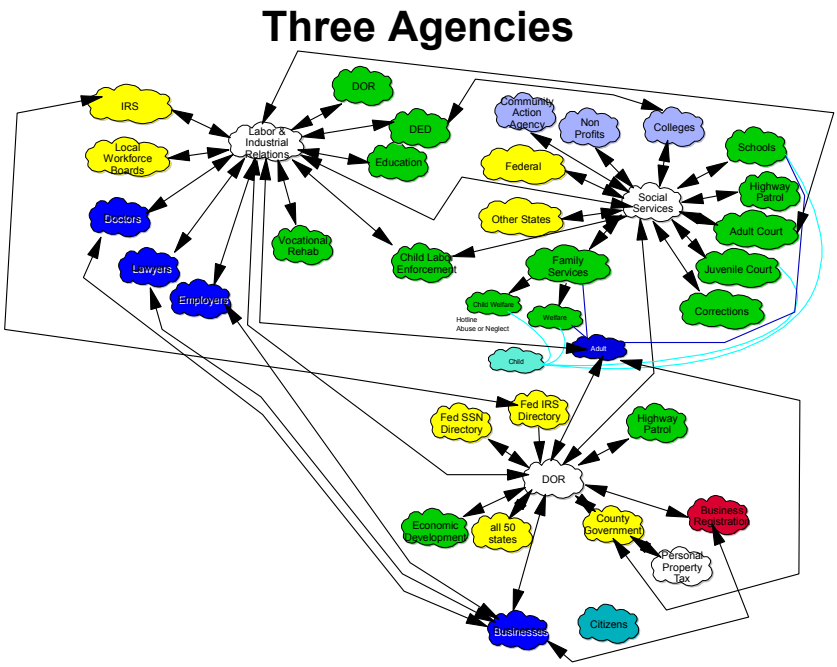


Figure 6

What becomes obvious is that there are a multitude of relationships, not only between businesses and/or citizens and the state, but also between state agencies that are dealing at separate times with the same person or business. Over a dozen state agencies are identified in the diagram above.

One of the primary objectives repeatedly identified for state portals is that they should simplify the ease with which an individual can interact with state government. While technology can enable that, simple, citizen centric interactions will not occur without also addressing the process and organizational issues implied in the preceding picture.

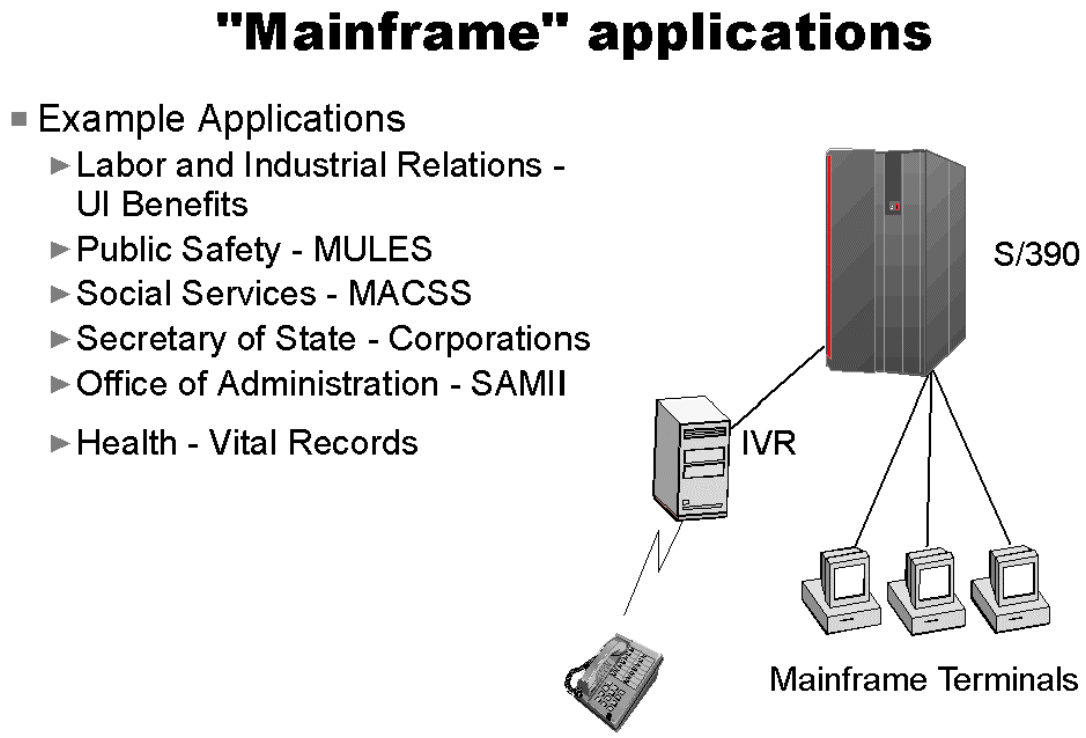
3.3 I/T Infrastructure

The State of Missouri has an extensive portfolio of I/T systems supporting its business functions. Those systems represent a considerable number of application models and operational environments.[4] The current I/T infrastructure is described in the following series of consolidated diagrams.

[4] Based on review the information provided by the State of Missouri, interviews with I/T management and IBM intellectual capital.

3.3.1 Mainframe

Several departments and elected officials have applications that run on the "mainframe". These generally support a large number of users. In addition to interactive applications (the majority operate under CICS) there is significant batch processing and large print volumes. The majority of the applications were developed to support requirements specific to the State of Missouri. Development was done either by state employees or under contract for services. Often the applications have been modified and enhanced over a very long period of time to support the changing requirements of the State of Missouri. This evolution over a long period of time generally makes it fairly difficult to change the applications.



The applications are written in procedural languages, with COBOL in use for the majority. A number of applications exist that utilize Assembler programs for specific functions. Several major applications are either deployed or under development using COOL:GEN. There are a variety of languages that comprise the remaining applications (i.e. FOCUS, EDA, MANTIS®, and COBOL-XT). The information is accessed using both flat file (typically VSAM) and database management systems (IDMS®, DB2®, SUPRA®).

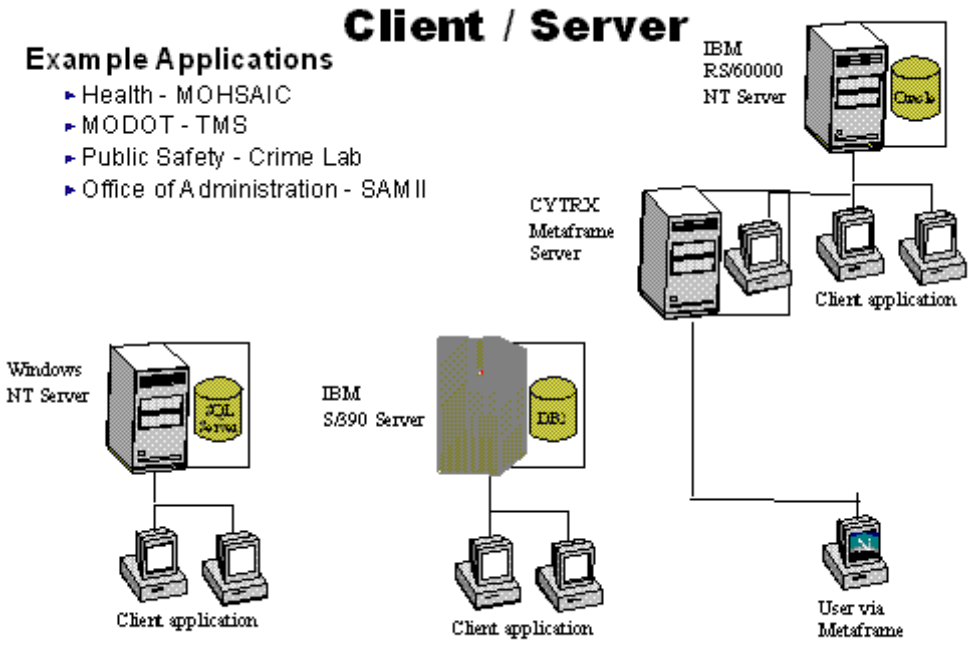
The users access the applications via terminals or through an Interactive Voice Response (IVR) that appears to the applications as a terminal. The communications between the terminal and the "mainframe" is very limited in size, requiring minimal network capacity.

Significant interfaces exist within these systems (i.e. Social Services common area) through a variety of techniques. Interfaces with other systems are generally batch file input or extracts, often using magnetic media (i.e. tape) on a periodic basis. Some custom interfaces have been developed to support specific requirements (i.e. MULES to Revenue).

3.3.2 Client / Server

Several departments and elected officials have applications that are "client / server". Some of the applications were developed to support requirements specific to the State of Missouri while others were commercially available (often requiring custom modification).

Users access the applications through programs that execute on their desktop computer (generally running Windows95, Windows98, or Windows NT). These programs are referred to as client applications. Some client applications can be access via a CYTRX Metaframe server. This opens access to a broader population of users by removing the need to actually execute the program on the user's desktop computer. This reduces the size of the client PC's but increases server and network demand.



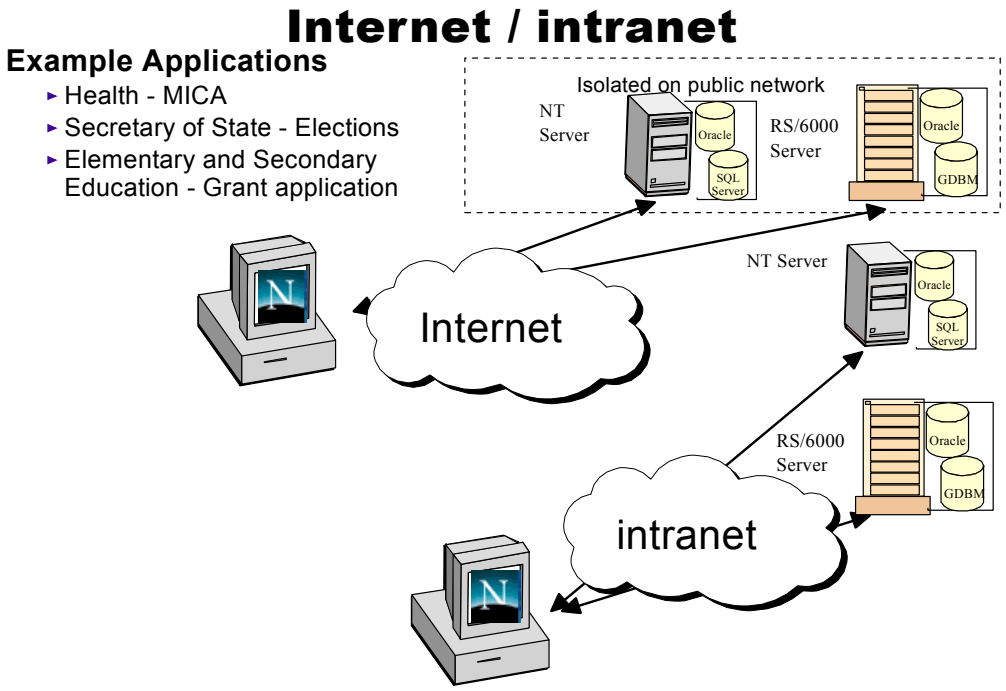
Server applications execute under a variety of operating environments. The three most common are Microsoft Windows NT®, IBM RS/6000®, and IBM OS/390®. A broad array of development tools and languages are in use, including Visual Basic, COOL:GEN, Delphi, Lotus Domino, Lotus Notes, C, C++, Visual Interdev and Microsoft Access. The information is generally accessed using database management systems (Microsoft SQL Server, Oracle, IBM DB2®).

The amount and nature of the communications between the client and the server applications vary between systems. Often significant network capacity is required. Interfaces with other systems are generally batch file input or extracts, often using file transfers over the network on a periodic basis. Other interfaces have been developed using specific tools such as IBI's EDA or IBM's MQ Series.

3.3.3 Internet / intranet

Most departments and elected officials have made some applications available to external users over the Internet or to internal users on departmental networks (intranet). Most of these applications provide either static content or allow the retrieval of information that has extracted from an operational system and placed on a server that is available on the Internet or intranet. A limited number of applications are available to users over the Internet or intranet that accept input and update operational systems.

Users access the applications through web browsers (i.e. Internet Explorer, Netscape) that communicate with the servers via HTTP. The servers are generally Microsoft Windows NT® running Microsoft IIS, Lotus Domino, or Apache Webserver. There are a number of IBM RS/6000® and SUN Solaris® systems running Apache Webserver. Among the most common tools are Front Page, Visual InterDev, COOL:GEN, and Lotus Domino.

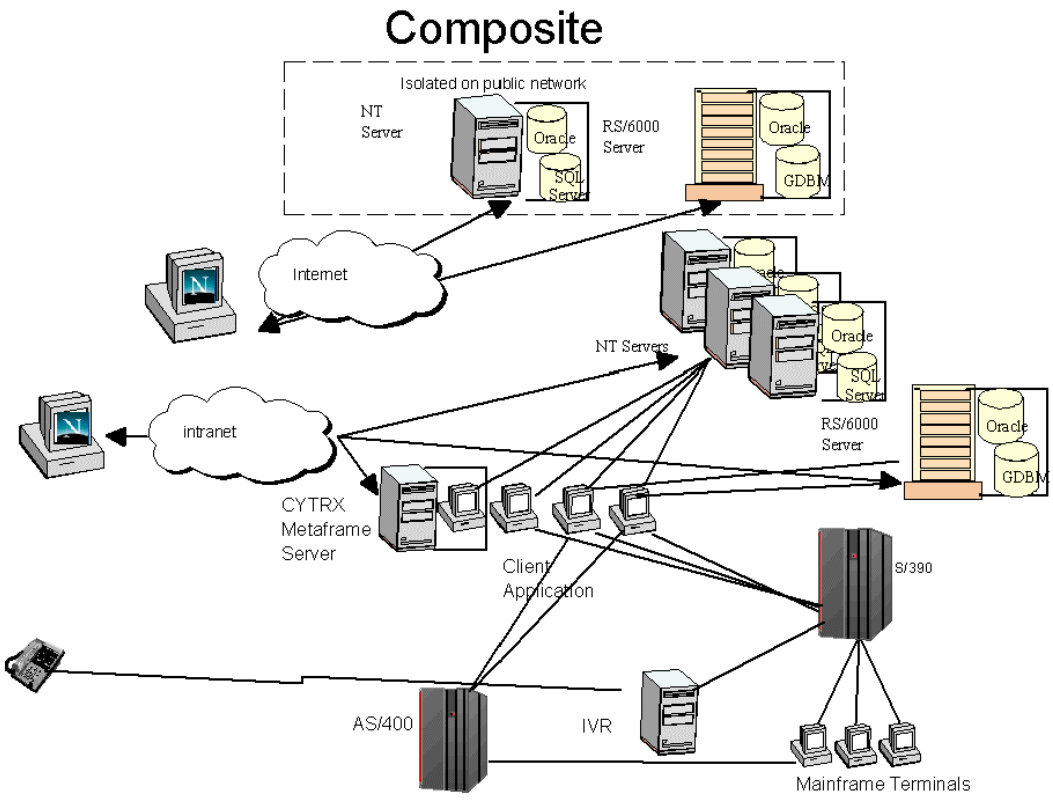


The scripting is done in a number of languages including C, C++, Java (limited), Visual Interdev and Microsoft Access. The information is generally accessed using database management systems (Microsoft SQL Server, Oracle).

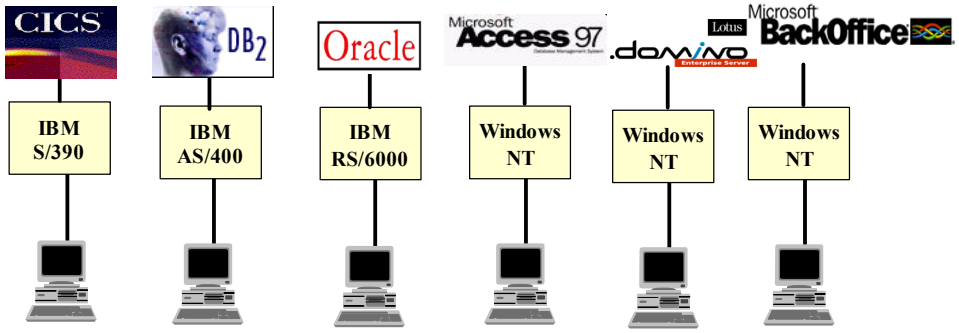
The amount and nature of the communications between the browser and the server often requires significant network capacity. Interfaces with other systems are generally batch file input or extracts using file transfers over the network on a periodic basis.

3.3.4 Composite View

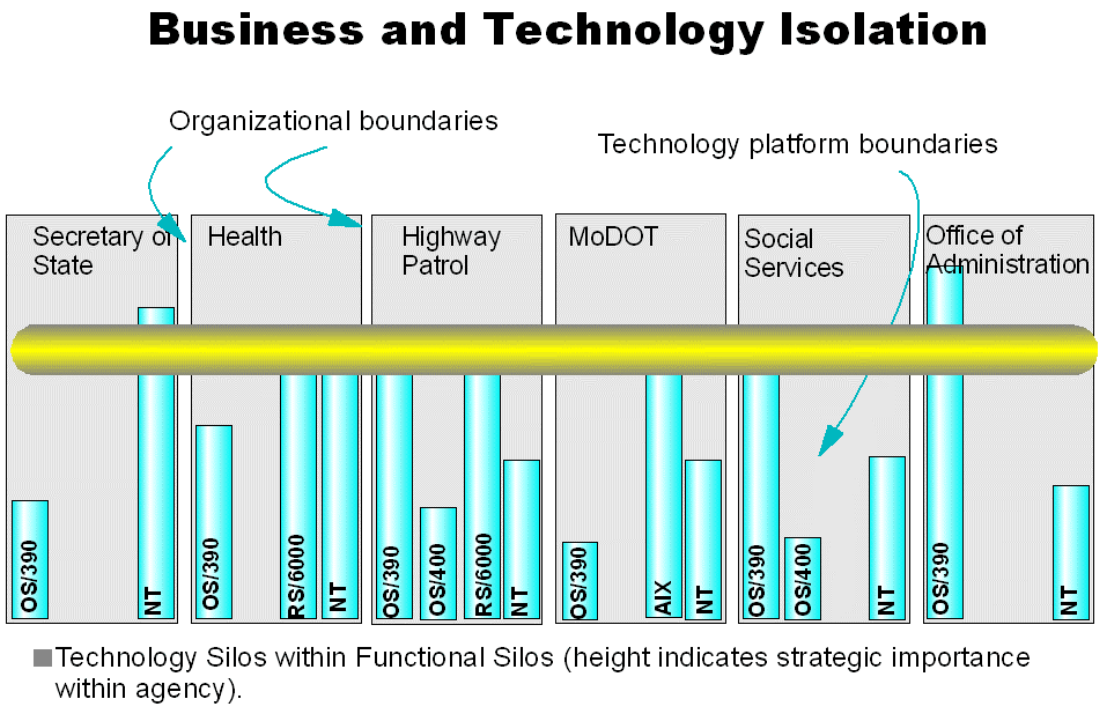
Taking a composite view of the I/T applications and infrastructure within the State of Missouri one readily sees that even a very simplified diagram becomes difficult to understand. The message to take from the diagram is that there are a significant number of programming models that exist across and within the state agencies. This results in a diverse operational environment (and requires a broad array of I/T skills).



The following diagrams depict a simplified view of the current enterprise application environment in place within the State of Missouri. As can be seen there are a number technology platforms in place. These platforms generally support independent "stove pipe" applications that have limited or no integration between them.



The resulting composite diagram takes selected agencies and places the technology platforms within them (combining similar platforms for simplicity). As can be seen there are both business (or organizational) boundaries and technology platform boundaries that will need to be addressed.



3.3.5 Summary

There are a number of differing application models in place within the State of Missouri. This is common for an organization that is as large and decentralized as the State of Missouri.

It is important to understand that while the number of different application models in place is increasing linearly, the number of potential application-to-application interfaces is increasing exponentially. This makes application delivery more cumbersome and decreases the resilience of installed systems.

4 Vision

To become an e-government the State of Missouri needs a comprehensive vision. There are hundreds of government services that are candidates for electronic delivery. These services must be integrated to reduce complexity, and delivered to the State of Missouri's constituents in a timely manner. This e-government architecture supports that comprehensive vision.
The State of Missouri vision is based upon an integrated point of comprehensive, ubiquitous, and useful access to government services, information (data), and people. It will support online communities of citizens, partners, businesses, employees and others in a variety of combinations.

4.1 Architecture Requirements

As depicted in Figure 7, Integrated Single Window, one of goals indicated by the State of Missouri is to provide a single window for citizens and businesses. This single window, or portal, should be able to deliver both multiple and cross-agency functions.

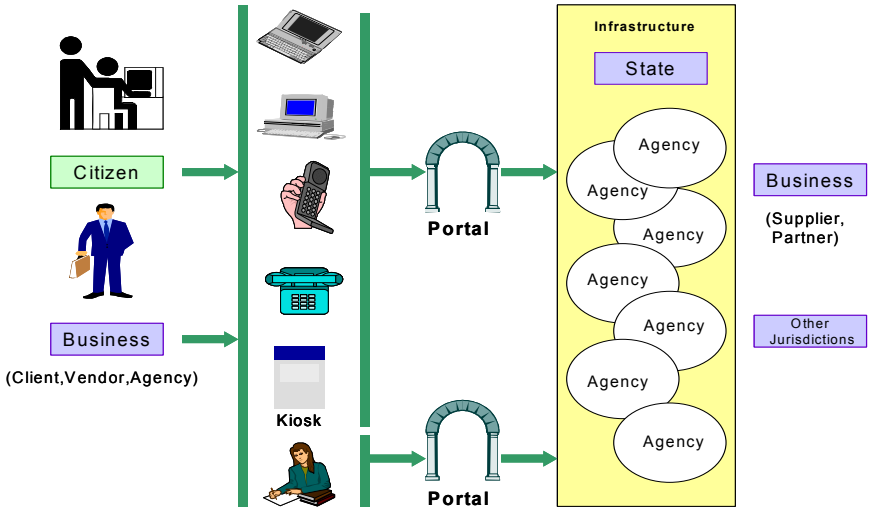


Figure 7, Integrated Single Window

The e-government architecture needs to be comprehensive, in order to support the extensive list of government services that are candidates for electronic delivery. It needs

to provide a framework that allows the State of Missouri to implement integrated services in the sequence that allows it to meet the priorities of its constituents.
There is a pragmatic limit to the resources that can be invested into e-government. This will require that services be delivered over a period of time. This will require a series of incremental steps. Each step should build upon the previous moving the State of Missouri towards its goal.

The State of Missouri has a vast inventory of I/T applications that support its business. These applications represent a tremendous investment. Many have been built over an extended period of time. The e-government architecture must allow for these applications to be an integral component.

As the State of Missouri implements e-government there is a need to provide adequate levels of privacy and security. The e-government architecture needs to support sound privacy practices, both business and technical. It also needs to provide appropriate measures to reduce vulnerabilities to inappropriate access to I/T resources.
The State of Missouri has common infrastructure in support of I/T (i.e. mainframe data center and telecommunications network). This common infrastructure needs to be extended to include the additional I/T components that are applicable within e-government. This will allow the agencies to leverage the activities and investments of other agencies.

The I/T applications within the State of Missouri typically have been designed and built independent of one another. They are built using dissimilar technologies and are specific to a given platform. Integration of them often proves difficult, if not impossible. The e-government architecture needs to be built upon a common reference architecture.
These requirements drive the e-government architecture. By following a systematic and consistent approach to building and deploying applications the State of Missouri will be better able yield the maximum benefit.

4.2 Architecture Recommendations

Missouri's e-government applications should be Web applications that leverage Web clients (such as Web browsers), Web application servers, and standard Internet protocols. The State of Missouri's e-government reference architecture is a Web architecture that is based on **open industry standards**. It allows selection among multiple implementation alternatives within the underlying architecture. The reference architecture provides support for integration with existing departmental applications, to leverage the state's I/T investments, and data from external non-Web services.

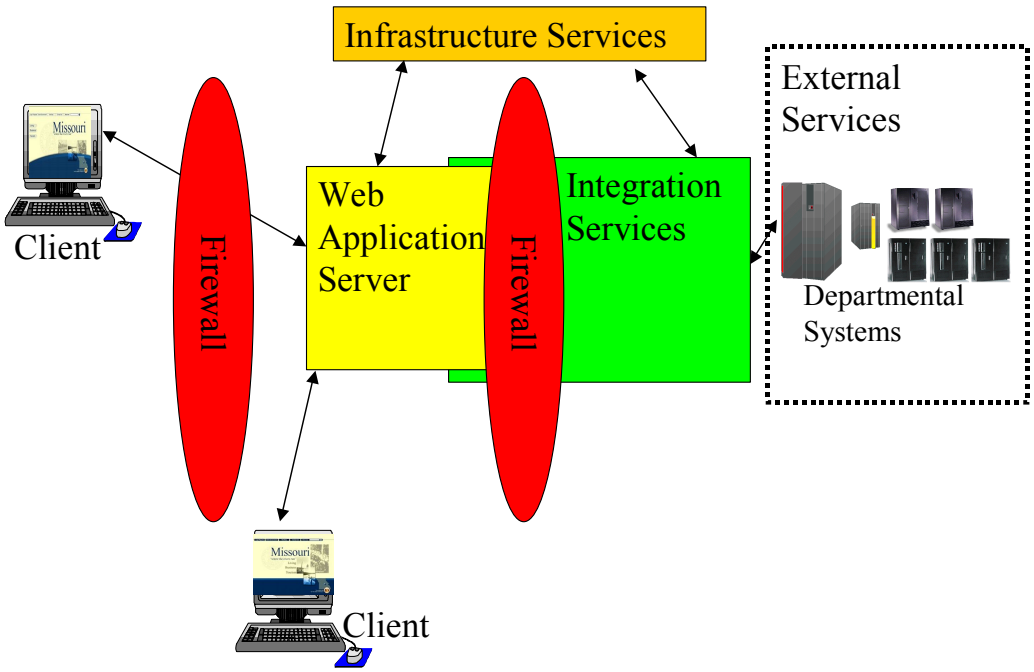


Figure 8, Missouri e-government Topology

Figure 8 illustrates the major elements of Missouri's e-government application topology. The topology consists of:

- Internet and intranet clients through which users communicate with Web application servers (using Internet standards such as TCP/IP, HTTP, and HTML) to access business logic and data. The primary role of the client is to accept and validate user input, and present results received from the Web application server to the user.
- Web application servers that are the hubs of the Web application topology processing requests from clients by orchestrating access to business logic and data on the server and returning Web pages composed from static and dynamic content back to the client. The Web application server provides a wide range of services for writing the business logic part of a Web application.
- Infrastructure services that provide the Web application server and its business logic components with directory, security, and other services. Included in these services are firewalls which shield an organization's network from exposure when connecting to the Internet, and prevent hackers and others from gaining unauthorized access to internal data, and computing resources.
- Integration services that provide support to Web-enable existing computing assets as well as to intelligently integrate business systems built on disparate architectures across the enterprise.
- External services that consist of existing, mission critical applications and data within Missouri government as well as external partner information services.

Most often these existing applications and services support the state's core business processes.

One of the key principles is that the business logic of a Web application always runs on the server and not on the client. Consequently, the key role of the client is to present results received from the application server to the user. The most common user interface (UI) model used in the Internet today is the HTML client, where the UI is driven from the Web application server. The UI can also be driven by part of the application that executes on the client, this application client model is used primarily in intranet environments.

Another key principle is the implementation of a clear and stable boundary between the business logic and the UI logic, allowing for independent development (and continuing modifications). Business logic are those elements of logic that actually record and process the user's input. The UI logic constructs the presentation and manages the interaction.

The value of abstraction and decoupling the user interface and business logic is widely recognized. For additional information there are a number of resources. One good source is *Design Patterns*, Gamma, Helm, Johnson, and Vlissides. Meta Group's *Infrastructure Agility* paper provides information about the need for an adaptive I/T infrastructure. Gartner Group's "*E-Business Is Driving a IT New Architecture*" highlights the architectural topics necessary to deliver e-government services.

The area in Figure 9 beneath the archway illustrates the operational architecture that enables the portal. Several aspects of the operational architecture should be noted:

- The separation of the network into zones to limit security exposure.
- The separation of informational and transactional web servers again to reduce security exposure.
- The common services provided within the interagency zone.
- The hub and spoke relationship between the web application infrastructure and the agency applications.

Development of this reference architecture for the State of Missouri's e-government implementation has been focused on the operational architecture. This operational architecture represents one of a complex set of interrelated architectures that need to be established. It is important to note that the value of these architectures is greatest when they are understood to be processes as opposed to artifacts.

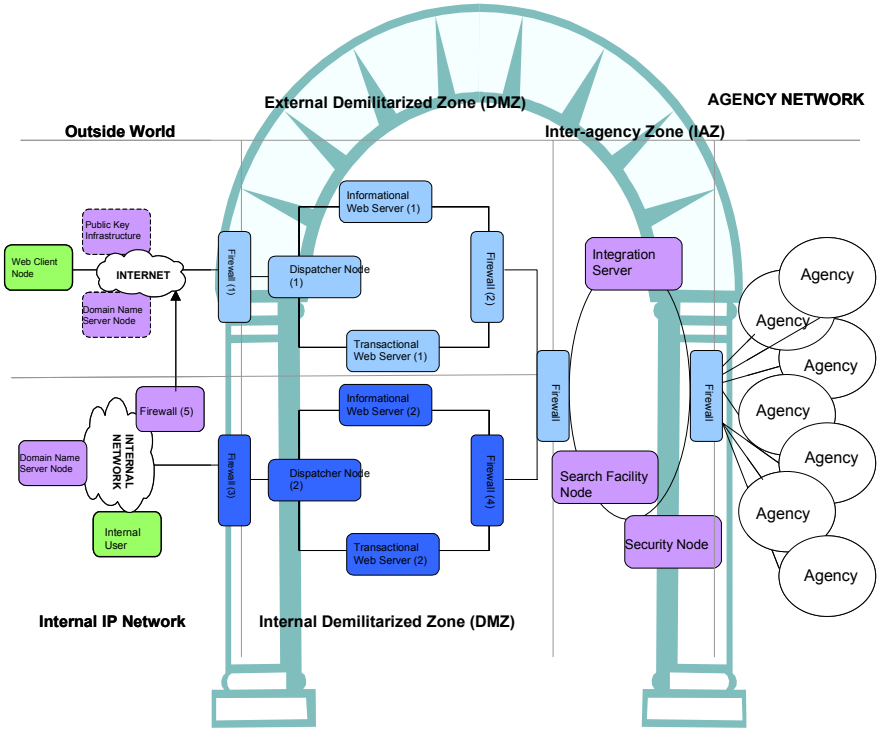


Figure 9, Operational Architecture

One way to look at the interrelated architectures is to use the proverbial "iceberg" depicted in Figure 10. The user sees only functional application and the user interface at the tip of the iceberg. I/T, depending on the paradigm that they view through, sees many more underlying components.

As expected, the base of the pyramid establishes long-term success. The base represents an awareness of the multiple architectures that are required to deliver the functions. Also it depicts the importance of a healthy architecture management process. Above the base is the operational architecture; a standards based approach to the delivery of application services. Above the application and integration architectures begin represent proven reusable designs that leverage prior successes. Above the architecture is the operation environment that supports the delivery of the business applications.

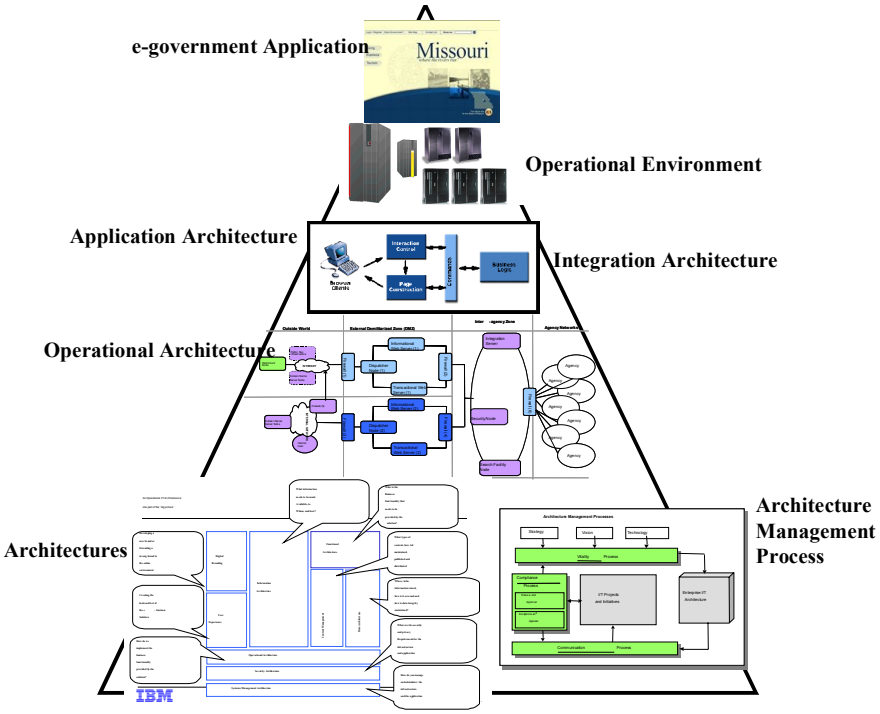


Figure 10

5 Gap Analysis

The State of Missouri has significant gaps that exist between the current environment and the targeted e-government architecture. These gaps are not uncommon as new approaches to the application of information technology are undertaken. The identified gaps are:

- Architecture principles are not completed. These principles define the underlying general rules and guidelines that the State of Missouri will use to invest in, use, deploy, and manage I/T resources and assets. These principles must encapsulate a fundamental consensus among the stakeholders.
- The State has not completed the definition and implementation of an architectural management framework. That framework needs to define necessary processes, roles and responsibilities in order to ensure the orderly on-going development and evolution of the State e-government I/T Architecture.
- The State has not completed the definition and elaboration of an enterprise-wide I/T architecture. This serves to leverage the I/T activities across multiple projects and departments.
- The State does not have a consistent model for integration of applications. This consistent model should define and document clear boundaries between systems.
- The State has a significant number of sites that have network bandwidth that will not be adequate to meet the requirements of e-government. This will need to be addressed to insure efficient delivery of services throughout Missouri State Government.

- The State of Missouri has not yet defined policies and procedures that establish the legal framework for a number of policy areas including digital signatures. This framework will need to be developed to realize the potential of e-government.
- The mix of I/T skills that exist within the State of Missouri will need to be evaluated. As job roles change, necessary skills will include the new technologies that comprise the e-government architecture.

6 Next Steps

Defining initiatives for Missouri must consider business and technology goals and issues. Listed below are the main strategic business results that the State of Missouri indicated they want to achieve through the use of e-business technologies.

- Improve Delivery of Services to Citizens and Business
- Increase Cost Efficiencies
- Invest in Partnerships
- Drive Economic Development

The initiatives described in the following pages are those that are primarily technology oriented. Those initiatives that are not primarily technology oriented will need to be identified and addressed outside of this project.
Some of these are likely to require senior executive decisions. For example;

- Allocation of funding and priorities for implementation of specific government services.
- The degree to which a common look and navigation model will be adopted (and enforced).
- The degree to which executive departments will have independent brands.

A process to determine what comprises an effective initiative begins by gathering information at the executive level and establishing a related value proposition. Concurrently with this the required capabilities and associated metrics that define success are defined. This is followed by considering whether each capability is a requirement of the **T**echnology, business **P**rocesses, or **O**rganization and culture of the enterprise. This analysis creates a table such as the following:

Goal	Targeted User	Value Proposition	Capability	PTO
Enhance Service				
	Citizen (please note that in this brief example, success criteria has not been identified)			
		Single Sign on		
			Common Security Policies	P[5]
			Common Security Interface	TO[6]
			Authentication Synchronization	PT[7]
			Single Administration Interface	PTO[8]
		Comprehensive Search		
		Personalized Content		
	Other Agency			
	Business			
	Non Profit			

This example shows that, for something as simple in concept as single sign on, that more than technology is required to support the citizen value proposition. That is, it must be determined what exactly a single sign on will grant access to the citizen. The process shown briefly above is a process to simultaneously identify and prioritize business initiatives and the technology on which they will depend.

6.1 Technology Initiatives

The significant technology initiatives that were determined to be appropriate (during the workshop) for Missouri to address are:

- Implement an Interagency Zone
- Embrace a Portal Framework

---

[5] This is a process requirement for the state in that those policies that are exposed to citizens have to be consistently managed across all state agencies. This requires that the policies be stated (documented), communicated, and agreed to in some form.

[6] The interface is technology, however it requires organizational support to be effective on behalf of the citizen. Without organizational buy in, the appearance of single sign on will not meet the potential of the technology.

[7] Authentication (how you identify yourself) has to be synchronized across multiple platforms so that the appearance of single sign on is made real. This requires identifying the necessary security policies and processes associated with each application, including support for audit and administration.

[8] A single security administration interface is required both by citizens (so that they remain unaware of the potentially disparate systems within state agencies which provide their services) and by the help desk supporting those citizens. This requires identifying the relevant processes in different agencies involved in security management, the organizations that are affected by single sign on, and the technology needed to implement this interface.

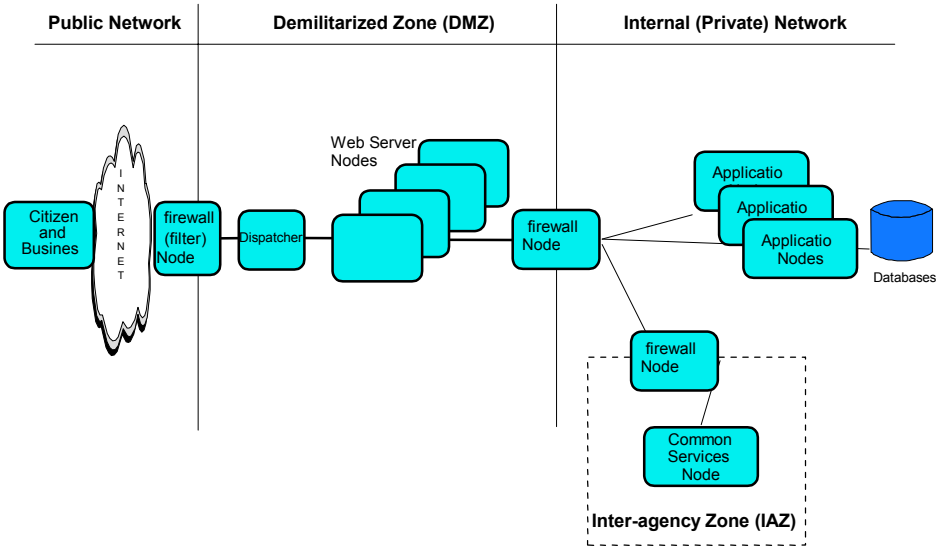
- Adopt Common User Authentication / Digital Signature
- Implement a Credit Card / Payment Gateway
- Adopt an Enterprise Application Integration architecture
- Define Common Commerce Services

These are not prioritized because the specific government service initiatives are still being identified. A prioritized government services initiative list is a necessary prerequisite to prioritizing the technology initiatives.

6.1.1 Implement an Interagency Zone

It is generally accepted that it is appropriate to implement a firewall configuration commonly referred to as a Demilitarized Zone (DMZ).[9] The DMZ is a (perimeter) network that is neither inside the private network nor part of the public (Internet) network. It serves to protect the resources in the internal network from the Internet. There are a number of services that will be required to support e-government. Many of those services can be provided by a common infrastructure. These services need to be protected from the Internet. Within the State of Missouri there are a number of independently managed private networks (with differing security implementations). Therefore these common services will need to be isolated from these independent networks. As shown in the following diagram, this isolated network will provide an Interagency Zone (IAZ). The IAZ will utilize a firewall configuration that isolates it from both the DMZ and the internal networks.

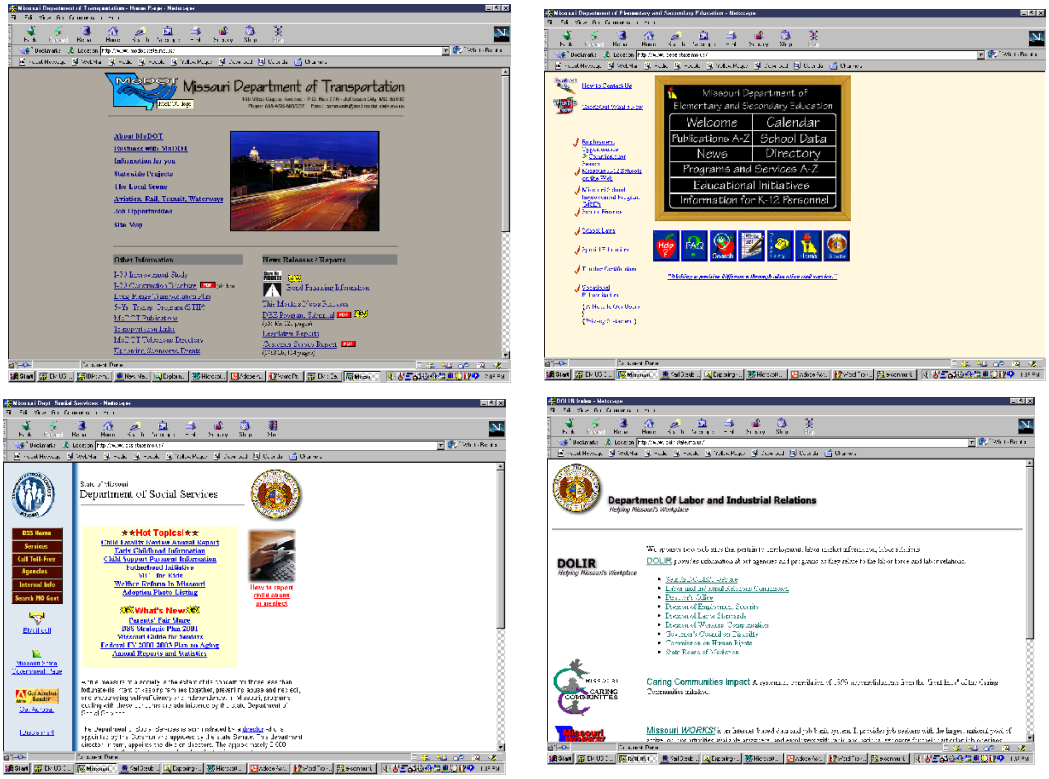
[9] A Demilitarized Zone (DMZ) is a type of firewall configuration that places your security software and hardware between two routers. The outer router controls traffic between the Internet and the DMZ, the inner router controls the traffic between the DMZ and the internal network. The job of the outer router is to filter out unwanted protocols and restrict inbound traffic to a limited set of IP addresses and ports. Because it only advertises the DMZ to the external network, external systems cannot reach the internal network. The inner router only permits access between the internal network and the DMZ, so internal systems cannot reach the Internet directly. The zone between these two routers is the DMZ, and in here you place the servers for the applications that you want available on the Internet, such as Web servers, proxy servers and socks servers. This is a very secure firewall configuration because an intruder must penetrate three separate systems to breach the firewall security.



6.1.2 Embrace a Portal Framework

The State of Missouri, and many other governments, has seen that the number of Internet users continues to exceed even the most optimistic estimates. The advantages of being on-line instead of "in line" are widely recognized. Most of the agencies have a presence on the Internet. The State of Missouri has established a home page at http://www.state.mo.us as seen below:

This home page serves as an entry into the State. Browsing this page indicates that the information is primarily arranged based on the organizational structure of the Missouri State government. The presence of that organization hierarchy has several implications. Finding information, services, and organizations often requires an understanding of which agency (or agencies) has the service. Lacking that knowledge, the search process is lengthened. This impacts both the customer and the state.



As seen by the images above of several of the agencies home pages, the look and user navigation models, while largely similar, are different. The use of color, HTML, Java, and JavaScript is inconsistent across the different sites. This is a common situation, one easy to understand. It does, however, make the appearance of integration more difficult. A statewide Portal framework can:

- Provide citizens, business, and others with simple, convenient and consistent access to Missouri government.
- Enable agencies to leverage the framework and implement e-government services more quickly and at a lower total cost.

Implementing a portal within the state environment will be more complex than just simply putting a new front end on the current environment. That said, the portal is likely to start out looking to both outsiders and to state personnel as just that: a new front end. An appropriate design point for the portal must be to enable the state to leverage their current investment while evolving to this new environment.

The portal should allow the state to target the information and services that they deliver to unique groups. Providing information and applications matched to a user's interests, roles, and needs is known as personalization. A personalized site is more likely to attract

and retain visitors. Personalized sites for employees improve their productivity by simplifying access to information and applications. Overall customer satisfaction is increased when less time is required to locate account information, and service is personalized to the customer's needs. One common reason for personalizing a site is to make the site easier to use. The State should not need to predefine all groups when the system is first designed.

To make this work, over time the current systems will need to move to a consistent model for offering applications and web content. Information searching will migrate from the provenance of the individual web server owners to the state. Again, this will benefit from increased consistency in application technology. Each of these will enable the state to move into e-government in a more flexible manner.

6.1.3 Adopt Common User Authentication and Digital Signature

It is vital for the State of Missouri to address the issues related to the security and privacy of information. One of the fundamental components of e-business is the capability for customers, employees, and others to work with an organization's resources over the Internet. As these new business practices emerge, most enterprises are finding that their existing security implementation is not capable of meeting the rapidly changing and more rigorous demands of doing e-business.

The state must assure the protection of proprietary and confidential information. This will require two fundamental security services: **authentication** and **authorization**. An individual (or even another computer) must first be authenticated before it can be determined if they have the authority for any requested access or operation. This does not prevent unauthorized parties from intercepting or even altering the information as it is in transit over the network. **Encryption** is a technology that can, if properly used, protect data from being disclosed to unauthorized parties.

When legal obligations are involved a means must be in place such that the creator of a document cannot later dispute the fact that they created that document. **Digital Signatures** are one potential way to address this requirement.

A statewide user authentication and digital signature initiative can:

- Provide citizens, business, and others with simple, convenient and consistent access to Missouri government.
- Enable agencies to leverage the initiative and implement e-government services more quickly and at a lower total cost.

Implementing a consistent user authentication within the state environment will be complex. It must allow the state to leverage their current investment while evolving to this new environment.

The state must continue to develop the legal and technical foundation to:

- Design and implement a consistent security framework.
- Determine how "Missouri Digital Signatures Act" will be implemented.
- Implement secured communication for sensitive information.

6.1.4 Implement a Credit Card / Payment Gateway

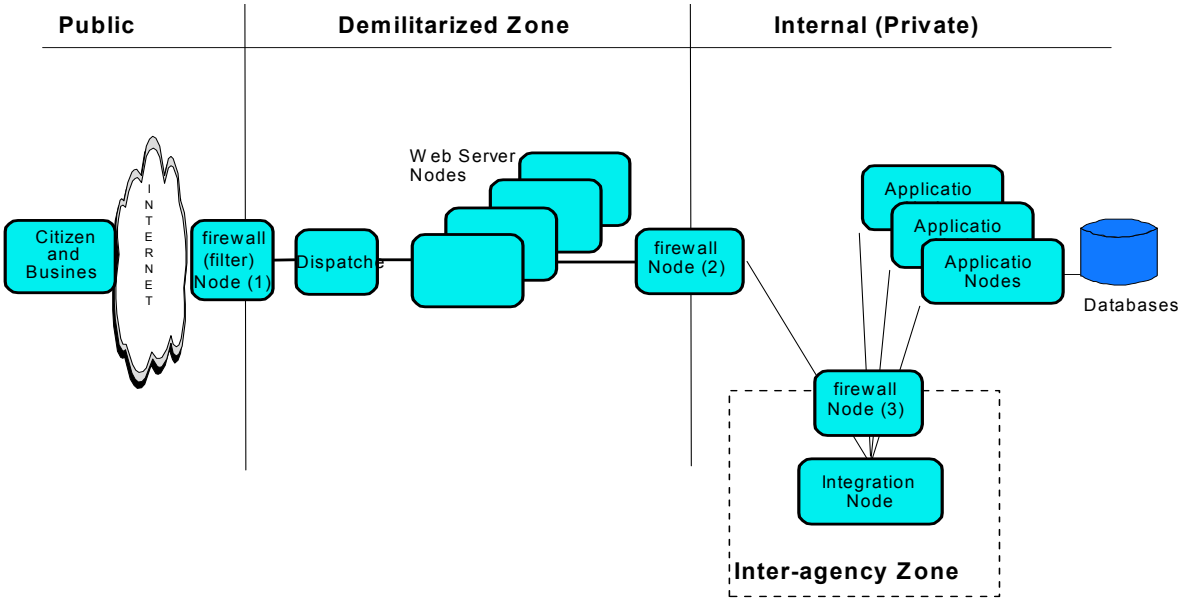
The State of Missouri clearly sees value in providing credit card convenience to its citizens and businesses. The Credit Card Initiative is intended to enable the state provide this capability creating an environment which combines technical flexibility and freedom for the state to redefine itself as needed as it becomes more and more of an e-government. Undertaking this initiative on a statewide basis can:

- Leverage the total revenue and transaction volumes of the state to obtain the best possible contract for credit card services.
- Wherever possible, develop credit card applications once and make them available for all agencies.
- Enable any interested agency to start using credit card services as soon as they desire.

It is likely that this initiative will require multiple phases. The first phase is a statewide implementation supporting "card present" transactions, allowing departments to accept credit cards. The second phase would implement common web services via common credit card interfaces (HTML, Applet, JavaScript) to be used by all agencies for credit card processing. The interfaces should generally include capabilities such as authentication, credit approval, credit denial. Further, this system needs to provide an interface so that credit card transaction information can be captured for central management by the state.

6.1.5 Adopt an Enterprise Application Integration Architecture

As indicated in the findings reviewed previously, implementation of comprehensive e-government applications will require integration across a variety of application models. To facilitate this an Enterprise Application Integration architecture is needed. On of the key components of this architecture is the Integration Server Node. It provides a 'front



end', or single point of access to the heterogeneous application servers. Through it access is provided to the many different departmental.
The Integration Server Node can provide a single view of multiple applications running on one or multiple hardware/software platforms. As such it extends and expands the value of existing applications, and eases implementation of e-government applications.
The Integration Server Node must deliver some fundamental functions:

- Isolation - of the various access point and legacy system protocols and formats
- Integration of various legacy services and information
- Automation of navigating among the various systems with flexible choreography
- Reuse of the existing legacy systems for new offerings
- Augmentation of existing systems by adding value (new processes, conditions) in the Integration Server Node

Undertaking this initiative on a statewide basis can:

- Allow the state to develop integrated e-government applications.
- Enable agencies to leverage the efforts of others allowing the implementation of services more quickly and at a lower total cost.

6.1.6 Define Common Commerce Services

Several of the agencies of the State of Missouri indicated that they have a need to offer goods or services for a fee and would like to make them available through the Internet. The Commerce Services Initiative addresses the need to provide services required in this commercial setting. These services potentially include:

- Order processing (including the shopping cart)
- Accept payment information and forward it to a payment gateway
- Process and forward shipping information
- Catalog access and management

Undertaking this initiative on a statewide basis can:

- Leverage the total revenue and transaction volumes of the state to obtain the best possible contract for commerce services.
- Allows commerce applications to be developed once and shared across agencies.
- Enable agencies to leverage the statewide commerce services and implement services more quickly and at a lower total cost.

The Commerce server may be housed inside within the State of Missouri's network (likely within the secure DMZ or the IAZ), or it may be outsourced and hosted by a service provider.

Part Four – Reference Architecture

1 Overview

This document describes a standard Logical Operational ***Reference Architecture*** for the Internet/Intranet Domain. This Reference Architecture has been developed and validated in diverse customer engagements by IBM. Each Node is described in detail, and a Walkthrough illustrates how the Nodes in the model function together.

The document also describes a Logical Operational Reference Model designed to address the e-government requirements of the State of Missouri. The Model represents an enhancement to the standard model; it incorporates enhancements designed to enable seamless delivery of functions across agency boundaries.

The reader should note that the models are at a 'logical' level , designed to describe the basic operational characteristics of the Internet/Intranet Domain. The models are at a level of abstraction that does not commit or constrain the State to specific products or vendors. Further elaboration of the model (i.e. mapping components to nodes, and defining the collaborations among components) would be an essential next step in developing product selection criteria and technology standards.

2 The Semantics of I/T Architecture

The architecture of an IT system is the structure or structures of the system, which comprise software and hardware components, the externally visible properties of those components, and the relationships among them.

In their 1996 book, Software Architecture: Perspectives on an Emerging Discipline, authors Shaw and Garlan observed that "It is now common practice to draw box-and-line diagrams that depict the architecture of a system, but no uniform meaning is yet associated with these diagrams."

While the I/T industry has recognized the problem, and there has recently been considerable convergence among recognized experts on architectural semantics, there are no single, universally recognized standards for architectural constructs, language or notation.

IBM Architecture Description Standard (ADS) is the 'dialect' used within this document.[10]The complete semantic model for ADS is very rigorous, and a complete discussion is beyond the scope of this document. The reader needs only to be comfortable with the basic architectural terms below in order to make use of the architectural 'artifacts' included in this document.

2.1 Architectural Constructs

The ***Functional Aspect of an I/T Architecture*** describes the ***function*** of the IT system and is primarily concerned with: the structure and modularity of the software components including:

- Interactions between components, including protocols
- Interfaces provided by components, and their usage
- Dynamic behavior, expressed as collaborations between components

The ***Operational Aspect of an I/T Architecture*** describes the ***operation*** of the IT system and is primarily concerned with:

- Representing network organization (hardware platforms, locations, topology, etc.)
- What runs where - where software and data are 'placed' on this network

A ***Component*** is a modular unit of functionality that eventually will make its functionality available through an interface. The functional aspects of a system are described primarily by specifying the collaboration that takes place among components.

Collaboration (among components) is a sequence of operations, identifying which components perform operations and which request operations, reflecting the time sequence. Collaborations are the primary way of modeling the dynamic behavior of components.

Use case scenarios are a unifying theme that runs through both functional and operational models. A use case scenario is realized in the functional model as collaboration between components, with a sequence of operations executed. This collaboration (based on the same scenario) can be represented as a ***walkthrough*** in the

[10] A standard for architecture description by R. Youngs, D. Redmond-Pyle, P. Spaas, and E. Kahan, **IBM Systems Journal Vol. 38, No. 1, 1999 - Enterprise Solutions Structure** (http://www.research.ibm.com/journal/sj38-1.html).

operational model to validate that the placed components can achieve required service levels.

A ***Node*** represents a hardware platform (at some level of abstraction), onto which components can be placed. The operational aspects of a system are described primarily by the placement of components on nodes, and the relationships among nodes

A ***Domain*** is a subject area that defines a context for analysis and description of some aspect of an I/T system. Specifically, a Domain is a set of: structural and behavioral patterns that describe some part of the architecture of an IT system (e.g., workflow, transactionality, user interface, network communications).

Reference Architecture is a proven pattern or template for a specific Domain. Successful I/T Architects and Organizations over time develop repositories of successful models for one or more Domains. By using and re-using ***proven*** Reference Architectures – architectures that have been validated through successful implementation, - system designers can significantly reduce the costs and risks associated with system design, development, and implementation.

The Reference Architecture is linked to the business context, by one or more ***Contextual Views.*** A Contextual View is an informal artifact that describes the purpose and/or requirements for which the Technical Reference Architecture is intended; these views are designed to communicate the essence of the proposed solution to non-technical stakeholders.

3 Contextual Views

The Views presented below provide a context for the Missouri e-government Architecture.

Figure 11, on page 49, illustrates the notion that citizens have multiple types of contact with the State of Missouri through their lives. Currently, the State does not have a single relationship with the Citizen, but multiple 'silo' relationships involving multiple channels, locations, and agencies. The citizen bears the burden of responsibility for identifying and coordinating these relationships for any particular event or life phase. These relationships can be quite complex, such as the steps required to establish and operate a small business.

The 'vision' is to provide 'client-focused' business systems and processes, which provide the citizen with a single view of State Government – one that significantly reduces the need for the citizen to understand the underlying structure of the State Government. A very straightforward example would enable Citizens to provide a single address change that would then be propagated across all agencies and reflected in all government records. Both the State and Citizen benefit by replacing multiple, redundant, error-prone processes with a single transaction, which ensures that the relationship is based on timely, accurate, and consistent information.

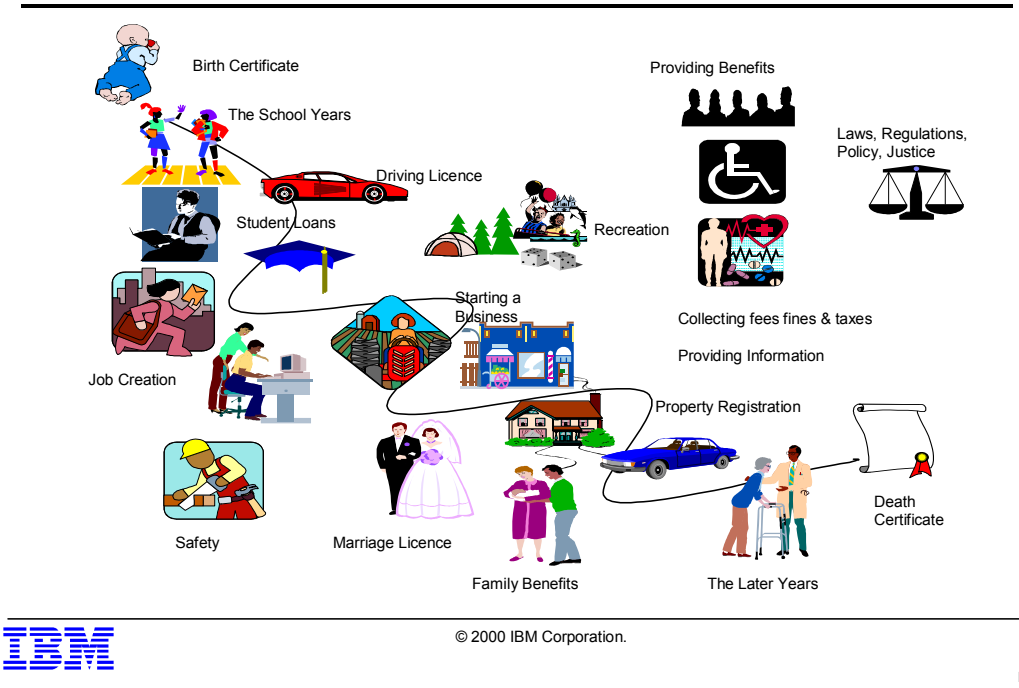


Figure 11 - Client Focus

Figure 12, on page 49, illustrates how the World-Wide Web (as well as traditional and complementary channels) could enable this type of single window to the State.

By developing and implementing a set of 'common business functions" accessible by State employees , and enabling access to those functions through the Web, or from other devices (such a telephones through Interactive Voice Response and Computer Telephony Integration, or IVR and CTI), the State could ensure that transactions or queries performed across multiple channels will produce consistent results.

A key feature of the view is that access is through a portal that is separate and distinct from the existing State Agency systems. The solution is structured as a separate agency-independent functional 'tier' that serves as a 'hub' for inter-agency integration.

'Hub' based architecture is significantly less complex than a collection of heterogeneous system-to-system connections. Mathematically, where ***n*** represents the number of interconnected systems a hub-centered system requires '***n*-1**' connections, while system-to-system coupling requires 'n^2 **–1**'. An exponential growth in connections is inherently more fragile, costly, and difficult to manage and maintain than the linear growth presented by a hub-based topology.

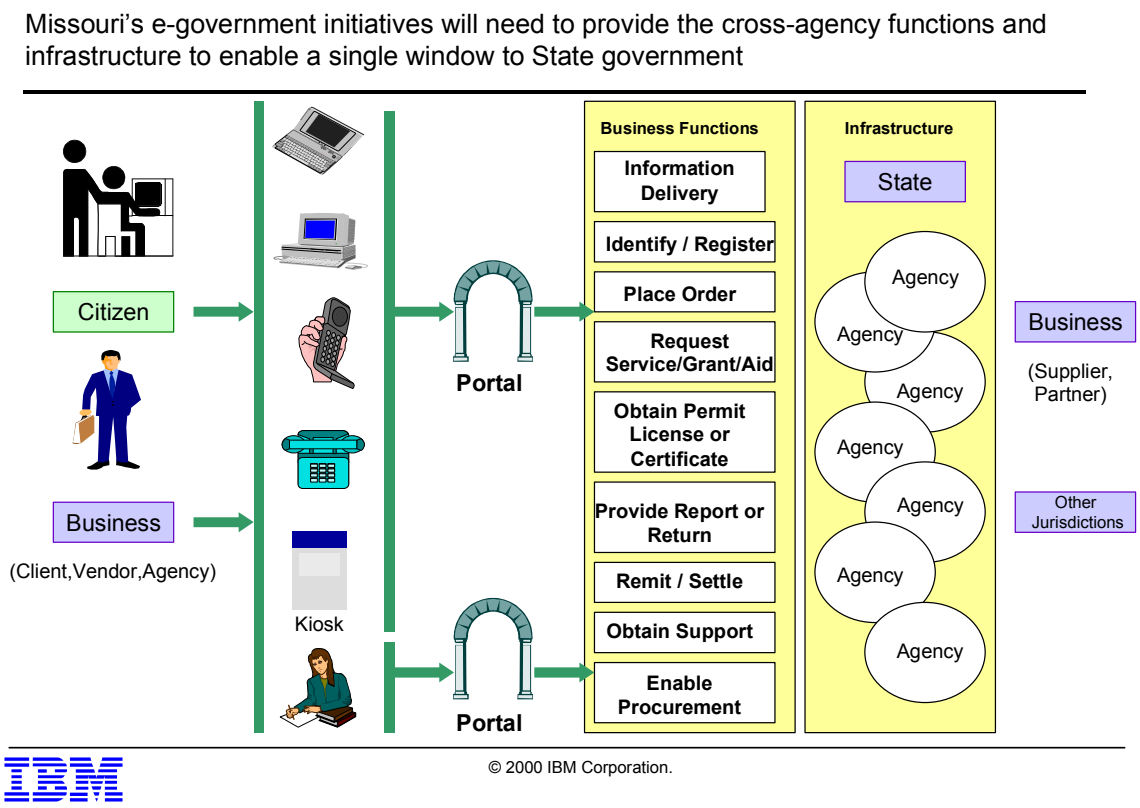


Figure 12 – An e-government Portal

4 Internet/Intranet Reference Model

4.1 Logical Operational Diagram

The standard Logical Operational Diagram for the Internet/Intranet Domain is presented in Figure 13, on page 51.

The most obvious feature of this architecture is the demarcation of the network into multiple zones, including:

- The external world

- A DMZ, or demilitarized zone which provides external (internet) access to State systems
- A second DMZ, or Demilitarized Zone, which provides internet (internal) access to State systems
- Internal (secure) zone

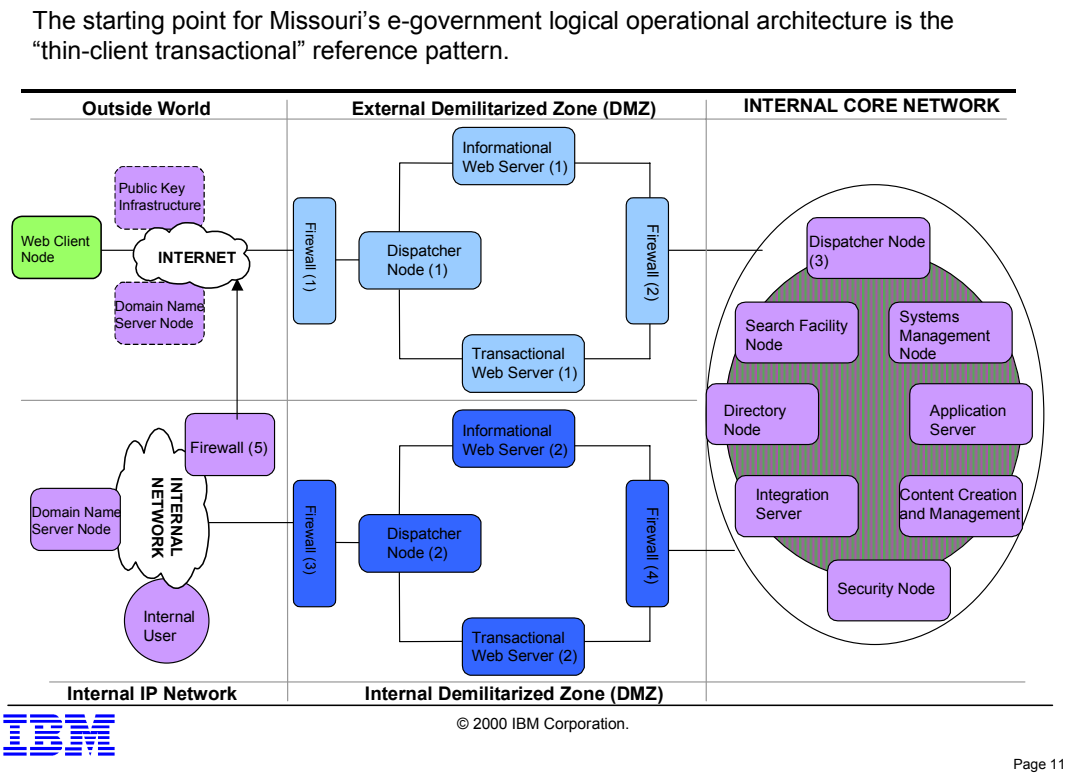


Figure 13 The Internet/Intranet Domain

The need for a Demilitarized Zone to isolate an Organization's I/T assets from Users on the Internet is well known and accepted in the industry. The State is sufficiently visible that it will be the subject of regular and persistent attacks, and without state-of-the-art security controls, is likely to sustain damage. The DMZ, demarcated by Firewalls, (as well as complementary security measures, such as monitoring and ethical hacking) is an essential structure for mitigating the risk of attack from the outside world.

A need for a separate and complementary DMZ is not as well recognized in the industry, but is strongly recommended since the open nature of the IP protocol makes it prone to intrusion and hacking. The intranet DMZ is essential because it assists in protecting the State's I/T assets since:

- Users may be connecting to the intranet from external, remote locations (e.g. dial-up VPN, business partners). This increases the changes of attempted entry from non-authorized users.
- Experience has shown that the majority of computer hacking and intrusion are done by an Organization's own employees.

The backend systems are shown as a collection of selected Nodes connected to an internal core network. The backend Nodes represent common systems running applications and holding data that have an enterprise-wide scope (i.e. are of interest to many users across the Organization). These backend systems may be accessed from the intranet as described later and they may also be accessed from other delivery channels.

Any individual Node in the intranet pattern may be duplicated for availability and/or load balancing reasons. The decision to duplicate a given Node should be taken at the detailed design phase.

The intranet Nodes may be replicated as a whole to support different user populations for service level and security reasons. For example, there may be one set of Nodes to support intranet applications for internal employees. There may be a separate "cloned" set of intranet Nodes, running different applications, for business partners. The principal reasons to replicate the intranet Nodes in this way are for service levels (e.g. ensure adequate performance and availability for a high-priority group) and for security (e.g. physical isolation of different applications and data to minimize intrusion possibilities).

4.2 Logical Nodes

4.2.1 Overview

These logical nodes are described on the following pages. On-line versions of this document provide hyper-links to the appropriate definition below.

- Application Server Node
- Content Creation and Management Server Node
- Directory Server Node
- Data Server Node
- Domain Name Server Node
- Firewall Server Node
- General Purpose Workstation Node
- Integration Server Node
- Kiosk Node

- Mail Relay Node
- Public Key Infrastructure Services
- Security Server Node
- Systems Management Node
- Voice Over IP Gateway
- Web Server Node - Informational
- Web Server Node - Transactional
- Workflow Server Node

4.2.2 Application Server Node

The Application Server Node processes business applications that do not run on a single-user workstation. Typically applications are placed on an application server because the application data is shared between many people who may wish to use the application simultaneously. Typically these applications have a division-wide or enterprise-wide reach and use large and very active databases.

Application Server Nodes might be implemented on the following platforms, e.g. S/390, AS/400, SUN, RS/6000, Intel, etc.

The Application Server Node(s) generally processes all of the business logic for the application and all of the data access logic. The databases accessed by the application may also reside on the application server, or may reside on a separate data server node.

The Application Server Node may also process some of the presentation and application navigation logic. A special case of this is an application written for use on a "Green Screen" using 3270, 5250 or VT100 protocols, where the Application Server will process all of the presentation and navigation logic.

Where an application has been written to use a GUI, it is likely that all the presentation logic and maybe some of the navigation logic will be processed at the workstation.

The Application Server implements a transactional model of computing to allow multiple users to access and update the same data with integrity. Transactions must be managed by a transaction manager such as CICS or by a database manager with transaction management capabilities. If a single transaction updates resources on more than one server, the transaction managers involved must also implement a mechanism for two-phase commit.

A client can initiate a transaction on an Application Server using either a synchronous interface such as RPC or an asynchronous messaging interface. Most application servers will also have to perform batch processing initiated automatically by a batch-scheduling tool.

4.2.3 Content Creation and Management Server Node

This Node serves two main purposes - the creation of content destined for the Web servers and the overall management and distribution of that content.

On the creation using the services of this Node can produce side, new content, and changes to existing content. This Node is responsible for the creation of content that is destined for the Web Informational and Transaction servers. This includes HTML pages, forms, Java script, XML documents or other forms of documents that are to be published to the Web servers. It can also include Web pages with document attachments and forms.

This Node is not responsible for the creation or management of configuration files, installation files, setup files or information destined for Nodes other than the Web servers.

The content management functions of this Node include the overall change control of the created or updated content and the publishing of that content to the Web servers.

This Node can act as a container for versions of Java applets that are linked to the Web server content and will carry out the necessary management and distribution functions to publish the Java applets to the Web servers. However the Java applets are developed elsewhere - they are brought together with content for final integration testing and distribution. The Java applets life cycle (from design to user acceptance test) must be kept intact and be in addition to the content management carried out by this Node.

4.2.4 Directory Server Node

The Directory manages a company-wide directory structure. This can generally be implemented as either a single, centralized corporate directory server or as multiple co-operating directory servers. If multiple, they may be cascaded in a hierarchical relationship or they may house partitioned replicas of parts of the corporate directory information.

The Directory maintains information about the characteristics of potentially any resource or entity on the network (servers, data stores, applications, meeting rooms, users, customers, suppliers, etc.). The characteristics maintained about each resource would typically include information such as its name, network address and creation data. At the limit, all attributes that need to be known for a particular resource could exist in the directory. In this way the directory works as an insulation layer between the logical access to a resource and its physical characteristics.

To implement a common company-wide directory structure it is necessary to employ a variety of Directory Services and data. Common Directory Service processes include:

- Directory Administration: the managing and updating of directory entries

- Directory Search Engine: a facility for supporting the search and access to the Directory contents
- General Directory Applications: canned business applications that report on Directory information

4.2.5 Data Server Node

This node holds the components, which manage the data, which is created, updated and otherwise used by the company's operational systems. It may include operational data from other companies, which they are willing to share - for instance by EDI from a partner, or data sold as a service (that is - someone else's operational data).

The data server hosts both formatted and unformatted data. It is the source from which data is extracted for inclusion in the Data Warehouse.

4.2.6 Domain Name Server Node

The Domain Name Server Node provides the technology platform to provide host to IP address mapping, that is, to allow for the translation of names (referred to as URLs) into IP addresses and vice versa.

The Domain Name Server is part of a distributed Domain Name system database. Specific database segments are locally controlled, yet data in each segment is available across the entire network through a client-server scheme. Domain Name Servers contain information about some segment of the database and make it available to clients, called resolvers.

Resolvers are the clients that access name servers. They query the name server, interpret its response and return the information to the program that requested it. Resolvers vary in their level of sophistication. The most typical implementation is the stub resolver, which is quite simple and puts most of the burden of the resolution process on the name server. A full resolver, on the other hand, has more function and can off-load processing from the name server by performing tasks such as caching responses for future use (i.e. the next time the address for that name is requested, the resolver does not need to ask the name server).

4.2.7 Firewall Server Node

The specific security services / components that run on the firewall are:

- Packet filtering
- Socks
- Proxy
- Relay (DNS and SMTP)

- secure IP tunneling

Firewalls demarcate the "demilitarized zone. Firewall (1)Firewall (1) separates the outside world from the DMZ, and Firewall (2) separates the DMZ from the enterprise's internal network.

Firewall (1) is typically implemented with packet filtering which restricts outside access to a specific number of protocols and can also provide traffic screening based on factors such as:

- Where the traffic is coming from (source address)
- Where the traffic is going (destination address).

In this scenario, both HTTP (port 80) and SSL (port 443) are allowed through the firewall.

- HTTP is a non-secure protocol and is used for communicating with the Informational Web Server node.
- SSL, a secure protocol, provides encryption and authentication, and is used for traffic into the Transactional Web Server Node.

Firewall (2)'s primary role is as a filter to ensure source and destination addresses are the only ones allowed. It is also potentially used to protect the internal network (which may itself contain IP segments) from unauthorized access. In addition to firewall (1) functions it may have security services such as packet examination or packet relay (to break a direct connection between the secure web presentation node and the Integration Server Node).

General considerations to keep in mind in firewall design include:

- Implementation and maintenance of firewalls can be in-house or outsourced from an ISP
- Adherence to standards such as IPsec may be important if heterogeneous networks need to be integrated via mechanisms such as secure IP tunneling
- Understanding the level of logging required, as different firewall implementations greatly vary in this area (e.g. application gateway products typically offer more logging capabilities than routers)
- Defining the process to maintain and administer the firewall including:
  - Keeping it as simple as possible to minimize human errors
  - Securing the maintenance environment appropriately
- Understand the pros and cons of similar mechanisms such as socks and proxy. For instance:

- It may not be easy to find socksified clients for some protocols
- In general, proxies offer more extensive logging capabilities
- The performance impact of proxies is greater than socks as they involve more protocol processing overhead (proxies operate at the application protocol layer, while socks operates at the TCP/IP layer)
- Inbound sessions are not addressed by socks (from the non-secured network to a trusted server) since it does not provide for secure password delivery
- Web caching is not provided by socks (a Web proxy does) and therefore it may impact performance

Designing a security system involves a series of trade-offs involving the level of security, performance and cost. For example, deciding whether to use four small simple routers or one large complex router in a firewall will involve some of the following considerations:

- The simpler the router configuration, the easier it is to verify and change it (thus decreasing the risk of human error);
- The larger the number of devices, the more configurations need to be verified;
- More complex devices often provide more performance capabilities;
- Complex devices are typically more expensive and more difficult to replace;
- Four routers would offer more flexibility in terms of designing the network topology (which could be exploited to increase the level of security by providing more isolation).

4.2.8 General Purpose Workstation Client Node

The General Purpose Workstation represents the workstation requirements of typical users, not using particularly complex applications or a particularly large number of concurrent applications.

The workstation provides the man-machine interface for the business and service applications. The business applications are used typically through a GUI. Service applications refer to technology services, either visible to the user as with e-mail or office tools, or transparent to the user as with an RPC service or time services.

The general-purpose workstation can support various different application models.

In a Client-Server **model** it will support the presentation logic, probably some of the business logic, and possibly some of the data access logic. (There are several different Client-Server models that implement different splits between client and server).

In a Thin Client **model** it will use a web browser, possibly with embedded Java virtual machine. It will support part of the presentation logic as it interprets HTML and runs imbedded JavaScripts and/or applets. The Web Server will perform part of the presentation logic, as it builds dynamic HTML datastreams. The client may also perform some simple business logic (e.g. field validation).

In a Green-Screen **application model** the client will execute none of the application presentation, business or data logic but will just display the data stream sent to it.

4.2.9 Integration Server Node

The purpose of the Integration Server Node is to provide a 'front end', or single point of access to Application Nodes. Access is provided for many types of users as illustrated in the diagram.

The Integration Server Node can provide a single view of multiple applications running on perhaps multiple hardware/software platforms. As such it may extend and expand the value of existing applications, and ease the implementation of new applications. The Integration Server Node must deliver some fundamental functions:

- Isolation - of the various access point and legacy system protocols and formats
- Integration of various legacy services and information
- Automation of navigating among the various systems with flexible choreography
- Reuse of the existing legacy systems for new offerings
- Augmentation of existing systems by adding value (new processes, conditions) in the Integration Server Node

Important components that may be present on the Integration Server include:

- Message handler
- Decomposition/composition
- Navigation
- Transaction Management
- Connection/Session (State) Management

4.2.10 Kiosk Client Node

The Kiosk is a Node that can be implemented in various locations and with different communication characteristics (completely stand-alone, permanently connected, or connected on demand).

A standalone kiosk would have a multimedia player of some sort, such as videodisk, that is used to present different marketing or other messages to the prospect/customer, typically under the person's control through a touch-screen. Simple calculation-type applications may also be available.

The connected kiosk can also have a multimedia player, but also has interactive data and sound or video. This connection may be to a computer system, such as an IVR or even the Integration or Application Server Node, or on demand.

4.2.11 Mail Relay Server Node

The function of the Mail Relay is to reside in the DMZ and break the connection from the Internet users to the Internal Mail systems of the organization.

The Mail Relay communicates with all external users.

Only the Mail Relay can communicate through the firewall to the Mail Message Switch in the internal network via SMTP, and it can ONLY communicate to the Mail Message Switch on the internal network, nowhere else.

The value of this configuration is to mask the internal structure of the mail network from the outside networks. This is especially important if there are multiple mail servers communicating with the outside world.

Virus scanning may be implemented; the server scans all incoming and outgoing mail from the Internet for viruses on the mail relay. (This does not eliminate the risk of bringing in virus but does reduce it. The only way to eliminate the risk is to not allow attachments.)

(If a virus scan for outbound is required, then it should be implemented on the mail relay, not on the message. - If it's on the message switch, then it will scan every piece of mail including internal mail, which is typically not required.)

Another class of filtering which may be provided is Bozo Filtering, in which e-mail from specific external addresses is disallowed (i.e. not relayed). The addresses are those of chronic senders of unwanted and vexatious e-mail (known as spamming or flaming). The list of addresses (a “kill list”) is generally compiled based on User complaints.

4.2.12 Public Key Infrastructure Services

The public key infrastructure implements the technology to provide a binding between a public key and an identity through certificates signed by a certificate authority.

A Certificate Authority (CA) is a trusted entity that issues certificates. It may be external, such as a bank, or internal, such as an IS organization which acts as a CA for an enterprise.

An individual wishing to send an encrypted message applies for a digital certificate from a Certificate Authority (CA). The CA issues an encrypted digital certificate containing the applicant's public key and a variety of other identification information. Certificates typically contain:

- Name of the Owner and their public key
- Name and (digital) signature of the Certificate Authority
- An expiration date and serial number

The CA makes its own public key readily available through the Internet.

The recipient of an encrypted message uses the CA's public key to decode the digital certificate attached to the message, verifies it as issued by the CA and then obtains the sender's public key and identification information held within the certificate. With this information, the recipient can send an encrypted reply.

The most widely used standard for digital certificates is X.509.

4.2.13 Security Server Node

The Security Node provides security management functions such as:

- Identification and Authentication
- Key Management
- Audit Services
- Certificate Management
- Mapping between security schemes
- Intrusion Detection

Several areas of guidance regarding security are provided below:

(1) Establish Zones of Control

The enterprise should establish and recognize "zones of control", and then establish an appropriate level of monitoring and controlling access from outside the Company's own zone of control.

The concept of Zones of Control attempts to define groups over which an organization can reasonably assume they can expect predictable behavior. This can apply to different

groups, such as those deriving their income exclusively from the organization, or to a collection of systems and components in a network, such as an internal network or a demilitarized zone.

A company's zone of control includes anybody whose income depends exclusively on that company. By definition, anybody in this zone of control is referred to as "trusted". Those outside the company's zone of control are referred to as "untrusted" and their access should be monitored and controlled more tightly.

Authenticated and non-authenticated services should be separated, as non-authenticated service users are by definition outside the zone of control.

(2) Identify security relevant platforms and treat them as more sensitive than other platforms.

A security relevant platform is any system that:

- Has direct access from another zone of control (e.g. the outside world) or
- Controls access from another zone of control.

The security of the firewalls is paramount as all other network security depends upon them.

(3) Establish a DMZ

The concept of a DeMilitarized Zone (DMZ) is very important whenever outsiders are permitted access to an organization's network:

Any publicly accessible system, no matter how well secured, must be assumed to be breakable, as it may be subject to:

- Operating system weaknesses
- Configuration problems
- Administration problems
- Protocol weaknesses (e.g. UDP)
- Common application weaknesses (e.g. sendmail)
- In-house application weaknesses (e.g. CGI scripts)

Therefore:

- Put publicly accessible systems in a DMZ isolated from the internal "trusted" network.
- The systems in the DMZ should contain no sensitive or critical information.

- If a system in the DMZ is broken into, it should not be useable as a launching pad for attacks on the internal systems. Therefore, the internal network should be firewalled from the DMZ.
- Depending on the complexity of the DMZ and the systems in it, it may be necessary to place a firewall between it and the outside world. At least, there should be a filtering router between the two.
- Separate firewalls are recommended for inbound and outbound access in order to keep firewall configuration as simple as possible:
    - Inbound traffic rules are normally dynamic and complex, while outbound traffic ones are typically simpler.
    - Complex firewall configurations are more prone to human error and therefore increase the risk of break-ins.
- Consider standardizing on one firewall product. Although there may be technical reasons for using multiple products, maintenance and administration would be greatly simplified if only one product were used.
- To the greatest extent possible, limit application services to one per platform.
- Whenever publicly accessible systems are involved (e.g. services running in the DeMilitarized Zone), application services should be limited to one per platform to the greatest extent possible. Benefits of this approach include:
- Simplicity of configuration, which in turn brings about easier maintenance and administration, thus minimizing the risk of human errors; a weakness in one application will not compromise other applications.

(4) Consider separating the Web server function into two physical parts: an Informational one and a Transactional one:

An Informational Web server serves Web pages to the general public, does not require authentication of users, and does not have access to back-end systems. This server is the most likely to be attacked, as it is open to the outside world. The whole purpose of this server is for it to be accessible by anyone.

A Transactional Web server serves a subset of the outside world, requires user authentication, and has access to and knows how to get to back-end systems in the trusted network.

Separating the transactional and the informational environments would help minimize the risk to the transactional Web server, which is the one that can potentially be used to break into the back-end systems.

Integration and Application servers should be placed in the trusted network, as these generally contain sensitive or critical information, and know how to talk to other back-end systems.

(5) Limit points of access to the Organization's zone of control.

All external maintenance access points should be turned off except when the supplier needs it and with the knowledge of the company (e.g., on scheduled maintenance times or in the event of a problem).

Anyone with privileged access to a device should be subject to stricter authentication than normal users. Examples of additional controls that could be implemented include:

- Longer passwords
- One time passwords
- Smart cards
- Hand-held tokens

(6) Ensure passswords and/or PINS are suitably robust.

It should be noted that the PIN number commonly used IVR and Web applications is only 4 digits long, for a total of 10,000 combinations. This means that, on average, 5,000 guesses would yield the PIN number. This might be acceptable in an ATM scenario, where the intruder requires physical possession of the card, or even in an IVR application, where PIN guessing cannot be automated. But it is somewhat short for a web-based transaction application where knowledge of the card number is adequate and PIN guessing can be automated. A better recommendation is that PIN numbers be at least 6 to 8 characters long and not limited to numeric characters

(7) Limit employee access to information on the basis of need-to-know.

In an organization, one of the most important justifications for good security is to protect the confidentiality of customer information

In a Call Center context for example, a company's reputation could be severely compromised by a violation of customer confidentiality and privacy. To minimize this risk, the company should establish a business policy to define what customer information a Call Center or other employees can and cannot see (e.g., do CSRs require access to a customer's Social Insurance Number, and if they do, under which circumstances?). The risk associated with this issue is the violation of corporate policy and provincial/state/federal laws.

Technical mechanisms that could be used to prevent inappropriate data access, or to detect it if it occurs include:

- Real-time controls at the application level (e.g., when access to data is requested, the system could check for an active call for that particular customer, and only process the data access request if a call is actually in process).

- Automated log data analysis (e.g. processing log records after the fact to

4.2.14 Systems Management Node

The Systems Management Node represents the collection of systems management processes and data necessary to implement centralized systems management. This Node acts as an initiator and central collection point for all systems management activities (e.g. collection of alerts, polling of the devices reporting on trend data). This Node may be implemented as a single Systems Management Server or multiple Systems Management Servers cascaded in a hierarchical structure.

The business logic in this Node supports the systems management processes. Major focus areas identified by a typical company are:

- Operations Management
- Change Management
- Customer Satisfaction and Service Level Agreement (SLA) Management
- Problem Management
- Availability Management
- Backup/Recovery Management

The Systems Management Node is an architectural model, which is typically implemented as purchased packages from vendors (such as the Tivoli software).

Systems Management typically consists of a "managing" Node, with Client Function or (agents) running on the other Nodes that are to be "managed".

4.2.15 Voice Over IP Gateway (VOIP) Server Node

This node provides coding of (analog) voice into data which can be transmitted over an IP network, and provides decoding of encoded voice data into (analog) voice.

Tele-web collaboration typically involves a client, using a web browser, while talking to a Customer Service Representative at the same time. Although the voice conversation could take place over the telephone network, customers who use dial-up access to the Internet would require a second voice line. Alternatively, voice can be transmitted over the Internet to and from clients equipped with the appropriate computer hardware and Internet telephony software, using a single connection.

Using the Internet to transmit voice to and from the customer provides several advantages, including:

- Enabling customers with a single phone line to obtain voice assistance while using the same phone line to access the internet; the CSR can "walk" a customer through a transaction as it takes place;
- Allowing the customer to directly invoke telephone assistance from the browser (a single interface)

By translating digital signals to analog, and vice versa, the gateway would enables a Call Center to use the same infrastructure and equipment (PBX/ACD, IVR, telephone headsets and telephone controls) for calls placed through the internet and for calls placed through the Public Switched Telephone Network.

The reader should note that a complete discussion of the Call Center Domain is beyond the scope of this engagement.

4.2.16 Web Server Node – Informational

The Informational Web Server Node provides the technology platform to support access to information by users employing Web browser technology. The Informational Web Server can be used either:

- As a public web server connected to the public Internet.
- As a private, internal web server connected to the State's internal Intranet only.

For security reasons the web server will be positioned in a "demilitarized zone" of the network, separated by a firewall from the Internet or Intranet on the one hand and from the State's core networks on the other.

Data that is contained on the Informational Web server node would include

- HTML text pages to be downloaded to the client browser,
- Images to be included on the HTML pages,
- Multimedia content files to be downloaded, Application Program Library e.g. Java Applets for dynamic download to Client Workstation

This data is a read-only, operational copy of the master version of the data, which is created, stored and managed on the content creation and management Node. This data is replicated onto this Node for operational purposes only.

Although this Node can provide the management of hypermedia documents and diverse application function, the preferred approach is to have it provide page storage, retrieval and serving services only. Content creation and management should be kept on a separate Node (the Content Creation and Management Node). Application services, particularly those requiring a high degree of security, should be provided by the Transactional Web Server Node, in concert with the back-end Application and Integration Nodes.

4.2.17 Web Server Node – Transactional

The transactional web server Node provides the technology platform to support access to internal information by users employing Web browser technology. It is similar to the informational web server and provides many of the same services. However, in addition to these services, the transactional web server provides robust services to allow users to communicate with shared back-end integration and application systems. In this way it acts as an interface to business function, as opposed to implementing those functions on this Node.

This Node would be provided inside the enterprise network and inside a demilitarized zone for security reasons. In most cases, access to this server would be in secure mode, using services such as SSL or IPSEC.

Although this Node can provide the management of hypermedia documents and diverse application function, the preferred approach is to have it provide page storage, page retrieval, page serving and transaction passing services only. Content creation and management should be kept on the Content Creation and Management Node. Complex application services would be provided by back-end Integration and Application Nodes.

4.3 Domain Walkthroughs

4.3.1 Introduction

The Internet/Intranet Reference Architecture is illustrated in Figure 13, on Page 51.

Key collaborations through this Domain are as follows:

- The way Web Browsers and Web Servers interact to deliver pages of information to the desktop
- The ways of making web interactions secure
- The ways of achieving transactional characteristics over the web
- The ways to achieve integration with other domains

4.3.2 Internet Logical Operational Walkthrough

.4.3.2.1 Basic Operation from an External Internet Client

1. From an external Internet client (browser), a user will choose to link to a destination (URL) by typing it in, or clicking on a saved "favorite link", or clicking an imbedded link on the page that is currently displayed.

The link provides a name that must be resolved into a specific network address.

2. The address of that link will be found either in local cache on the client, or from a name server on the Internet (Domain Name System). The function of the name server is to provide the network address of a URL (or resource server).

If the default name server cannot find the address, then it typically would search other name servers until the address is resolved.

This is an area of uncertainty when it comes to performance since for the public Internet there may be an unknown number of searches performed to resolve the address .

3. Once the address of the specified link has been found, a message will be sent to firewall (1) to gain access to the Web Server Node, which is where the destination of that URL resides:

An Informational Web Server Node which serves Web pages to the general public, does not require authentication of users, and does not have access to back-end systems.

A Transactional Web Server Node which serves a subset of the outside world, requires user authentication, and has access to and knows how to get to back-end systems in the

trusted network. In this scenario the Security Node provides authentication.

4. Firewall (1) can use a number of schemes to restrict access from the Internet to the resources in the internal network (see details in firewall node description).

Firewall (1) is typically implemented as a filtering router, which restricts outside access to a specific number of protocols and can also provide traffic screening based on factors such as:

- Where the traffic is coming from (source address)
- Where the traffic is going (destination address).

In this scenario, both HTTP (port 80) and SSL (port 443) are being allowed through firewall(1):

HTTP is a non secure protocol and is used for communicating with the informational Web Node

SSL, a secure protocol, provides encryption and authentication, and is used for traffic into the transactional Web Node.

5. Once the request is allowed past firewall(1), it will be processed by the Web Node to retrieve a page of HTML text with embedded tags (e.g. for Images, Java applets, etc.).

If the request is going to the transactional Web Node, then the transactional Web Node may in turn communicate with the Integration or Application Nodes inside the trusted network (using an IP protocol) in order to process the request . In this case, additional security controls can be implemented at the application level on the Integration or Application Nodes (e.g. by using access control lists).

6. The information will flow back to the browser on the client workstation:

This may involve several interactions, since as the browser displays the HTML text, it may encounter tags causing it to load extra images, programs (applets), sounds, etc.

Downloaded applets can be digitally signed so that the browser can check their authenticity.

The performance may be unpredictable depending on the number and size of such downloads, the speed of the line, the load on the server, etc. (see Internet Design Guidance for more details).

7. Once an HTML form or an application (e.g. a Java applet) is downloaded to the client workstation, the user will then fill in whatever data is requested, and click the mouse a second time.

8. The message may flow either to the Web Server Node again, or it may flow directly to the Integration or Application Nodes. In the second scenario, the applet at the Web client will make a direct connection with the Application or Integration Nodes. This could be

illustrated in the diagram with the direct connection (on a predetermined port) between firewall(1) and firewall(2) for distributed object protocols.

The applet on the client can use a digital certificate to authenticate itself to the Integration or Application Nodes, and can also use SSL to encrypt the transmitted data. At the receiving end, an object will check the digital certificate, decrypt the message, and determine what methods the specific user is authorized to use (i.e. through access control lists). If any of these security checks are not successful, a denial of service will be returned to the client.

Any object on the Integration or Application Node could do the access control check. The check may only be done by the entry point objects, and bypassed for objects that are subsequently called by them, for efficiency.

There is a potential to use a proxy mechanism on firewall(2) in order to provide another layer of control (i.e. packet examination) before the packet is passed to the Integration or Application Nodes. Another way to provide this extra level of security would be by implementing a relay application in the DMZ that would break the communication between the Integration or Application Nodes and the Web browser.

9. The application program on the client (applet) can now communicate directly with the application on the Integration or Application Node (servlet). It is recommended in this architecture that minimal business function reside on the client in order to keep the size of the downloaded applet small. Function would reside on the Integration or Application Nodes where it can be shared and more easily managed. This is also recommended from a security perspective, as the less function an applet has, the less damage a hacker can potentially do.

This communication can be implemented using object approaches such as remote method invocation via protocols such as IIOP/SSL, RMI or DCOM.

10. Function or data needed by the Integration Node from back end application systems (i.e. from the Application Node) causes a message to be sent (likely via middleware, and over whatever protocol is needed, such as SNA to mainframes). This becomes normal client/server computing at this point, between the Integration Node and one or more back end systems.

Note that there may be a need to keep state (i.e. keep a position in the business transaction which links several atomic and unrelated requests from the client browser viewpoint). Middleware may be needed to assist. (Object Request Brokers, if used, provide some of the function required to keep state).

There may also be a need to manage a business transaction "unit of work" that spans several interactions with back end application systems. If this is the case then some "unit of work" or "transaction manager" service is needed.

11. The back end application system will access the requested business function and data and reply to the Integration Node that will forward the message back to the Internet client.

Note that the back end system may be an existing business application, or may in fact be a newly written system (e.g. to manage transactions and/or data on a corporate-wide basis).

12. If digital certificates are used by the application systems (e.g. to provide authentication), then a request will be sent to the Public Key Infrastructure (PKI) on the Internet to provide the required information (see description of digital certificates in the PKI Component Description). Please note that this assumes usage of a third-party Certificate Authority (e.g. Verisign)

4.3.3 Intranet Logical Operational Walkthrough

The following points illustrate the basic flow for an internal Intranet client accessing the company's business applications via the intranet Nodes.

1. Using an internal Intranet client browser, a user will choose to link to a destination (URL) by typing it in, or clicking on a saved "favorite link", or clicking an imbedded link on the page that is currently displayed.

The link provides a name that must be resolved into a specific network address.

2. The IP address of that link will be found either in local cache on the client, or from a name server on the intranet (Domain Name Server). The function of the name server is to provide the network address of a URL (or resource server).

If the default name server cannot find the address, then it typically would search other corporate name servers until the address is resolved (for more details see the component description of the Domain Name System.)

Performance for access to the intranet servers is more predictable than that of the Internet as resolution of server addresses will happen on the corporate intranet.

If the site specified is outside the corporate domain, then the request will be routed through the external web connection.

3. Once the address of the specified link has been found, a message will be sent to firewall (3) to gain access to the Web Node where the destination of that URL resides. (The Web Nodes in the DMZ are separated into informational and transactional nodes for security reasons:

An Informational Web Server Node that serves static and dynamic Web pages to users.

A Transactional Web Server Node that serves a subset of the user community and can access back-end systems in the trusted network for transaction processing activities.

User authentication may be required for all uses of the intranet, including those accessing the informational Web server. This is because authentication may be used to present the user with a tailored set of services, which he/she is authorized to use. In this scenario, the Security Node provides authentication.

4. Firewall (3) can use a number of schemes to restrict user access to the resources in the internal network (see details in the Node and component description of a firewall).

firewall(3) is typically implemented with packet filtering which restricts outside access to a specific number of protocols and can also provide traffic screening based on factors such as:

- where the traffic is coming from (source address)
- Where the traffic is going (destination address).

In this scenario, both HTTP (port 80) and SSL (port 443) are being allowed through firewall(3):

HTTP is a non secure protocol and is used for communicating with the informational Web Node

SSL, a secure protocol, provides encryption and authentication, and is used for traffic into the transactional Web Node. The third open port, used for distributed object protocols, is discussed further down in this flow. Other ports may be opened for Telnet, FTP, systems management, etc. if required.

5. Once the request is allowed past firewall(3), it may pass through a dispatcher, which is present for purposes of availability and load balancing across multiple Web servers. The dispatcher may not be initially required and may only be implemented once the transaction volumes grow.

The request will then be processed by a Web Server Node to retrieve a page of HTML text, which may have embedded tags (e.g. for Images, Java applets, etc.).

If the request is going to the transactional Web Node, then the transactional Web Node may in turn communicate with the Integration or Application Nodes inside the trusted network (using an IP protocol) in order to process the request. In this case, additional security controls can be implemented at the application level on the Integration or Application Nodes (e.g. by using access control lists from the Security Node).

6. The information will flow back to the browser on the client workstation:

This may involve several interactions, since as the browser displays the HTML text, it may encounter tags causing it to load extra images, programs (applets), sounds, etc.

Downloaded applets can be digitally signed so that the browser can check their authenticity.

The performance on the intranet will be more predictable than the Internet due to known end-to-end bandwidth, number of users, etc. The number and size of such downloads, the speed of the line, the load on the server, etc. (see Internet Guidance section for more details) will still impact performance.

7. Once an HTML form or an application (e.g. a Java applet) is downloaded to the client workstation, the user will then fill in whatever data is requested, and click the mouse again.

8. The message may flow either to the Web Node again, or it may flow directly to the Integration or Application Nodes. In the second scenario, the applet at the Web client may make a direct connection with the Application or Integration Nodes. This is illustrated on the diagram with the direct connection (on a predetermined port) between firewall(3) and firewall(4) for distributed object protocols.

The applet on the client can use a digital certificate to authenticate itself to the Integration or Application Nodes, and can also use SSL to encrypt the transmitted data. At the receiving end, an object will check the digital certificate, decrypt the message, and determine what methods the specific user is authorized to use (through access control lists on the security Node). If any of these security checks are not successful, a denial of service will be returned to the client.

Other authentication methods include Login ID and password, Java Ring (really a certificate), or by a smart card, etc.

Any object on the Integration or Application Node could do the access control check. The check may only be done by the entry point objects, and bypassed for objects that are subsequently called by them, for efficiency.

There is a potential to use a proxy mechanism on firewall(4) in order to provide another layer of control (i.e. packet examination) before the packet is passed to the Integration or Application Nodes. Another way to provide this extra level of security would be by implementing a relay application in the DMZ, which would break the communication between the Integration or Application Nodes and the Web browser. This could be a part of the function provided by the Transactional Web Server.

9. For the Internet, the size of a Java applet should be kept small because of limited bandwidth. For the intranet, if we have more predictable bandwidth and better control of the security implications of using an applet, the applet can be bigger.

This communication can be implemented using object / messaging approaches with protocols such as IIOP/SSL, RMI or DCOM.

Other packages may require other communications mechanisms such as Jolt to Tuxedo in the case of PeopleSoft. - this approach is tolerated but not encouraged.

10. If function or data is needed by the Integration Node from back end application systems (i.e. from the Application Node), then a message is sent (likely via middleware, and over whatever protocol is needed, such as SNA to mainframes). One of the reasons to have the integration server here is to do this protocol conversion. This becomes normal client/server computing at this point, between the Integration Node and one or more back end systems.

Note that there may be a need to keep state (i.e. keep a position in the business transaction which links several atomic and unrelated requests from the client browser viewpoint). Middleware within the integration server may be needed to assist this function. (Object Request Brokers, if used, can provide some of the function required to keep state).

There may also be a need to manage a business transaction "unit of work" that spans several interactions with back end application systems. If this is the case then some "unit of work" or "transaction manager" service is needed.

11. The back end application system will access the requested business function and data and reply to the Integration Node, which will forward the message back to the intranet client.

Note that the back end system may be an existing business application, or may in fact be a newly written system (e.g. to manage transactions and/or data on a corporate-wide basis).

The application system may not perform any business function and may only do protocol conversion or security checks.

12. If digital certificates are used by the application systems (e.g. to provide authentication), then a request will be sent to the Public Key Infrastructure (PKI - part of the security Node) to provide the required information (see security Node description and the component description s of digital certificates and PKI). Please note that this assumes usage of a third-party Certificate Authority (e.g. Verisign).

The remote dial-up users will gain access to the internal network through a private network dial-up connection. From an intranet point of view, these users will gain access to the intranet services the same way that local users do.

Firewall (5) is to allow access to the World Wide Web for Internet users and may also provide two-way FTP services to the Internet.

5 Missouri e-government I/T Model

5.1 Background

The State does not envisage strict central control of the design, development and implementation of Agency I/T systems; the scale and complexity of State government makes such strict central control unwieldy, impractical and ultimately unresponsive to the needs of its stakeholders.

The Chief Information Officer for the State will, however, encourage and sponsor the design, development and implementation of systems that will enable cross-agency inter-systems communications. These communications, will enable access to data or execution of transactions across Agency boundaries. An ‘InterAgency Zone’ of I/T infrastructure could, for example, provide the platforms and services required for cross-Agency processing.- whether such processing is initiated by internal systems, Users, or external clients through the Web.

5.2 The InterAgency Zone

Figure 14 on Page 75 illustrates the concept of an InterAgency Zone.

Key features of the architecture include:

- The zone is demarcated by a firewall that protects InterAgency systems from potential threats connected to Agency networks.
- The zone is protected from the Internet and intranet by DMZ's.

The most important Logical Node in the InterAgency Zone is the Integration Server; it enables isolation of the various access point and legacy system protocols and formats, and integration of Agency legacy services and information.

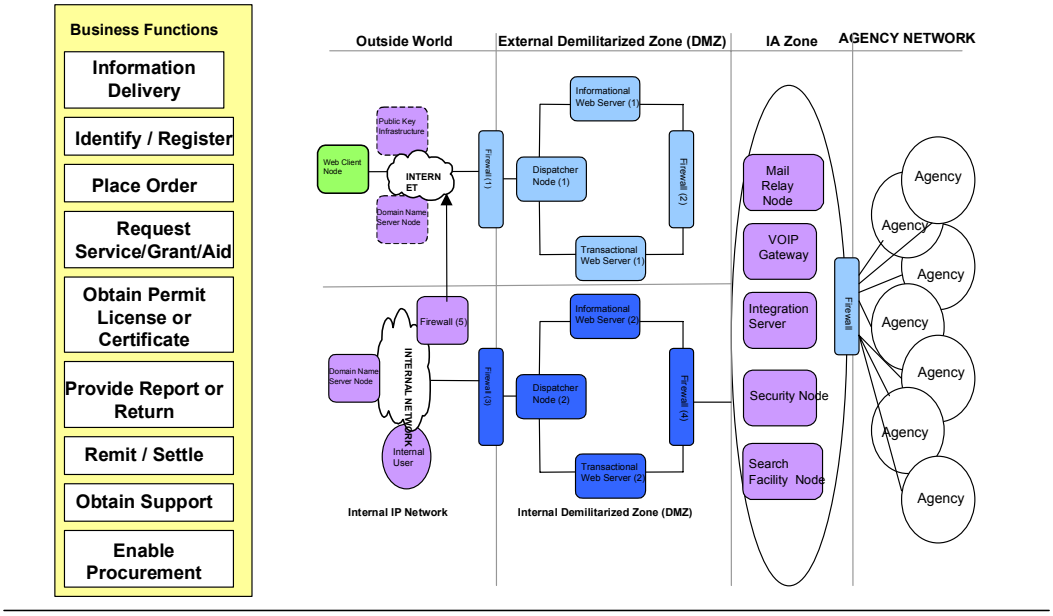
Message-oriented middleware can provide most of the communications between the integration server and agency systems. Although not suitable for all system-to-system communications, message-oriented middleware:

- Is (almost) universally available on all Agency platforms, and
- can be implemented with less impact that conversational or remote procedure connections between systems, since the only coupling between systems is based on a common 'understanding' of message content. The technologies of communicating platform are independent, since they are isolated through middleware.

Agency Application and Data Servers would remain in the Agency Zones.

Two Nodes have been added to the InterAgency Zone to ***illustrate*** the additional value the zone can provide by implementing services that are common requirements among multiple Agencies. These Nodes, the Voice Over IP Gateway and the Mail Relay Node, are described in detail in the section on Logical Nodes.

e-government initiatives will need to combine the delivery of function with the implementation of infrastructure, and the implementation of governance



© 2000 IBM Corporation.

Figure 14 – The Inter-Agency Zone

6 Architecture Management Process

The reader should note that the models presented in this document are not exhaustive. For example:

- The Internet/Intranet Domain models presented in this document are only the highest level of a complete Domain model, and only part of a complete Enterprise model. Additional Domains, and additional levels of detail (such as component descriptions, and detailed I/T walkthroughs for multiple scenarios) have been omitted for the sake of timeliness and clarity.
- Further additional architectural work will be required to develop technology selection criteria and technology standards before detailed systems design and development can begin.

The State will need to define and implement an Architectural Management Framework that defines the necessary processes, roles and responsibilities in order to ensure the orderly on-going development and evolution of the State e-government I/T Architecture

A high-level Architectural Management Framework is illustrated in Figure 15, on page 77; the constituent processes are described below:

6.1 Architectural Vitality Process

The Architectural Vitality Process is intended to ensure that the e-government I/T architecture is complete, current, and relevant on an ongoing basis. This process defines the processes required to complete and maintain the architecture as business and technology factors change – typically through regularly scheduled reviews and updates.

6.2 The Architectural Communications Process

The Communications Process is essential to ensure that there are effective means of communicating architectural requirements, constraints, and opportunities among the Agencies.

6.3 The Architectural Compliance Process

Through the Compliance Process, I/T projects are appropriately regularly reviewed for compliance with the architecture. Where non-compliance is an issue, mechanisms must be in place to ensure that projects are either brought into compliance or exempted through an Exceptions and Appeals sub-process of the Compliance process.

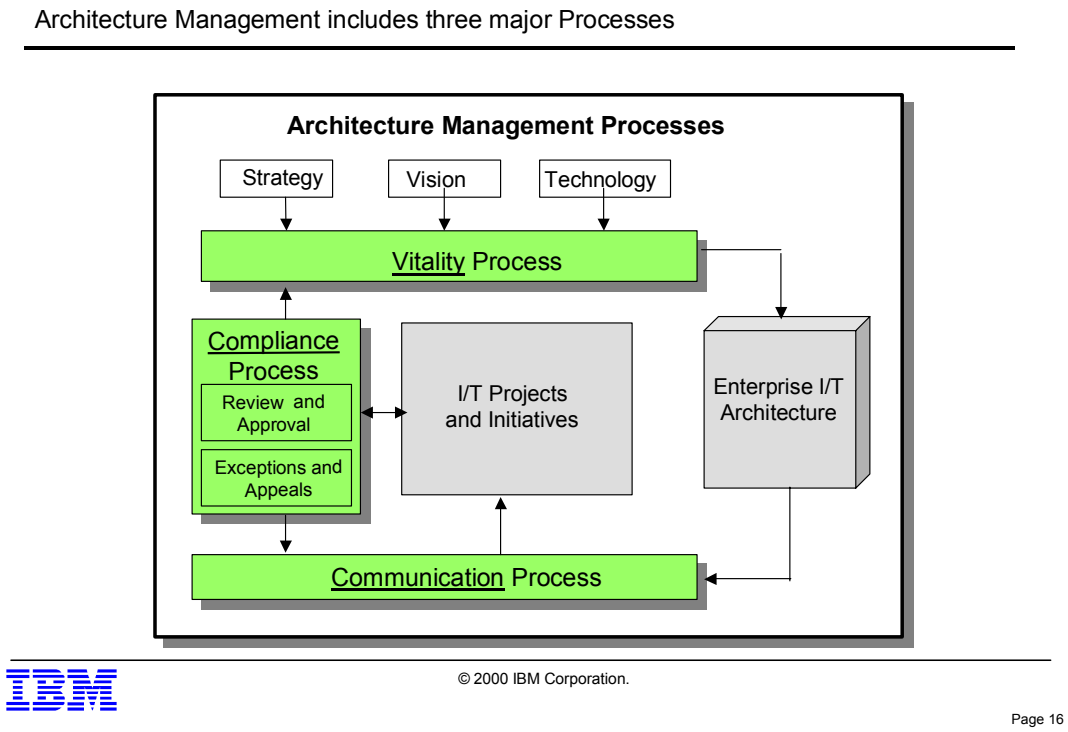


Figure 15 - Architectural Management Framework

Glossary

- **Access control:** Process of limiting access to the resources of an I/T product only to authorized users, programs, processes, systems, or other IT products.
- **ACID Principles:** The Atomicity, Consistency, Integrity and Durability principles which govern transaction management.
- **ACD (Automatic Call Distribution): A** function which allows calls to be directed to groups of call-takers based on call characteristics such as dialed number or calling line id.
- **ActiveX:** A component model from Microsoft which, for example, provides tools for linking desktop applications to the World Wide Web.

  Using a variety of programming tools--including Java, Visual Basic, and C++--developers can create interactive Web content. For instance, ActiveX technology can allow users to view Word and Excel documents directly in a browser.
- **Ad-hoc Reports:** Reports which enables transient or dynamic business decisions. The format, content, and timing of ad-hoc reports are dynamic. Compare Audit Reports and Control Reports.
- **Application Program Interface (API)**
  - The interface, or set of functions, between the application software and the application platform.
  - The means by which an application designer enters and retrieves information.
- **Application:** An application is a collection of automated functions in support of a one or more related business processes. Applications can span multiple business units, and multiple technology platforms.
- **Applet:** A small program designed to be executed from within another application. Unlike an application, applets cannot be executed directly from the operating system. A Java applet, for example, can only be executed under the control of the Java Virtual Machine.
- **Asynchronous:** An event that occurs at a time that is unrelated to or not dependent on the time at which another event occurs. The relationship between the time the events occur is unpredictable.
- **Architecture:** The structure of components, their interrelationships, and the principles and guidelines governing their design and evolution over time.
- **Architecture Model An** architecture model represents the structure and the relationships between the structural elements of a system. These models can either highlight particular areas of interest or represent an entire system. They do not only

represent the static relationships between the various parts of the system (static model) but also the way in which these parts interact to provide the desired functionality (dynamic model).

- **Architecture Principles: Statements** of intent or purpose related to the use of Information Technology within an enterprise. They describe preferred practices to be followed when implementing new or upgraded systems. They provide a foundation upon which the architecture model is built.
- **Asymmetric Encryption:** A type of encryption which uses one key to encrypt a message and another to decrypt the message. This differs from symmetric encryption, where the same key is used to encrypt and decrypt the message. Public-key systems are asymmetric.
- **Audit Reports:** Enable an independent reconstruction of sequence(s) of transactions, especially those pertaining to security, finance, or assets. Compare to Ad-Hoc Reports, and Control Reports.
- **Authentication:**
    - To verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system.
    - To verify the integrity of data that have been stored, transmitted, or otherwise exposed to possible unauthorized modification.
- **Availability:** The probability that system functional capabilities are ready for use by a user at any time, where all time is considered, including operations, repair, administration, and logistic time. Availability is further defined by system category for both routine and priority operations.
- **Bandwidth:** The capacity of a communications network.
- **Bozo Filter: A** filter which rejects e-mail from specific individuals base on its originating address. A feature supported by many e-mail clients and news readers. Bozo filters are used to ignore mail from chronic senders of unwanted, vexatious e-mail.
- **Browser:** Software that allows and facilitates access to the World Wide Web. As the user's gateway into the World Wide Web, Web browsers provide a client-based, end user environment for information delivery and interaction with Web servers. The two most common browsers are Netscape Navigator and Internet Explorer.
- **Business Management: A *Systems Management discipline*** which supports tasks encompassing a wide range of business and administrative functions for computer / network hardware, software and services.
- **Business System:** Hardware, software, policy statements, procedures and people which together implement a business function.

- **Bytecode:** A Java compiler creates platform-independent bytecodes that run inside of a Java Virtual Machine (JVM). That means that a Java applet can execute on any machine that supports a JVM.
- **Cache, Web A** Web cache sits between Web servers and one or more clients, and watches requests for HTML pages, images and files (collectively known as objects) come by, saving a copy for itself. Then, if there is another request for the same object, it will use the copy that it has, instead of asking the origin server for it again.

  Web caches can be either browser caches (serving a single client), or proxy caches (serving multiple clients).
- **Call Center:** A department that handles customer calls routed from an IVR.
- **Centrex (CENTRal office Exchange service):** a new type of PBX service in which switching occurs at the local telephone premises instead of on company premises. The telephone company owns and manages the communications equipment necessary to implement the PBX and then sells various services to the company.
- **Certificate Authority: A** Certificate Authority is a trusted entity that issues digital certificates. It may be external, such as a bank, or internal, such as an IS organization which acts as a CA for an enterprise.
- **Change Management: A *Systems Management discipline*** which provides the control and facilities to support the tasks of managing change in an information systems environment (e.g. planning, testing, approving, scheduling, distributing, synchronizing, installing, activating, and monitoring changes to hardware and software resources).
- **Client-Server:** Computing services which are partitioned into requesting processes (clients) and providing processes (servers), whether on the same platform or in a distributed environment.
- **Client:** As in client/server computing, the node which makes requests of the server.
- **Collaboration:** Collaboration occurs when two or more people participate in a business task that relies on the use of common information. Examples include meetings, document reviews, and sending, receiving and forwarding mail. Synchronous collaboration is the most common type of collaboration. Examples include audio/video conferencing and face-to-face meetings. Asynchronous collaboration removes time and location constraints. Copies of the collaboration document store can be spread over many locations.
- **Commercial (or 'Off-the-Shelf'): Any** item customarily used by the general public, that has been sold, leased, or licensed to the general public, or that has been offered for sale, lease or license to the general public.
- **Compliance:** A system is compliant with the architecture if it meets, or is implementing an approved plan to meet, all applicable architecture mandates.

- **Component Model: A** component model is a programming model that defines the syntax and semantics of interfaces for the creation, execution and management of software components. A component programming model (component model) consists of the syntax for defining interfaces and properties, for discovering or setting properties (introspection) and for discovering or invoking interfaces.

  These models specify how components interact at a technical level, i.e. no assumption whatsoever is made concerning the functional contents of these components. Or phrased differently, although these component models prescribe ways of finding out the actual (functional) Interface of a component, they do not prescribe in any way which functionality and to what level of granularity it is aggregated in them. For a component model, the actual functional Interface boils down to a number of strings representing the operations that can be invoked.

  The three most popular component models today are ActiveX (Microsoft), JavaBeans (Sun) and CORBA; the first two are mostly applied on the client and the last one is mostly applied on the server.

- **Component** A component can refer to any of the following hardware elements:
  - a part of a product (e.g. one of the executables that constitute the DB2/2 client for OS/2)
  - the part of the product that can be allocated to the client tier and server tier
  - a service

- **Compression, Data:** Storing data in a format that requires less space than usual. Data compression is particularly useful in communications because it enables devices to transmit the same amount of data in fewer bits. There are a variety of data compression techniques, but only a few have been standardized.

- **Configuration Management:** A ***Systems Management discipline*** which consists of facilities needed to perform the tasks associated with planning, developing, and maintaining the operational properties and their relationships.

- **Control Reports: Control** reports provide the data required to support the day to day operations of the business. Compare to Ad-Hoc Reports, and Audit Reports.

- **Conversational:** A type or model of program-to-program communication. Commonly used in the industry today and a wide variety of applications are based on this model. The model is described in terms of two applications that are speaking and listening-hence, the term conversation. A conversation is a logical connection between two programs that allows the programs to communicate with each other. Standards include CPI-C, APPC, and OSI TP. Contrast with RPC and messaging.

- **Configuration:** The specification of the exact parameters or settings to define hardware operation and connectivity. Can also be used for software set up.

- **CORBA (Common Object Request Broker Architecture): A** component model standard, established in 1991 by The Object Management Group, which provides a set of common interfaces through which object-oriented software can communicate.
- **COTS:** Commercial Off-the-Shelf. See Commercial.
- **CSR:** Customer Service Representative. An employee who takes (or originates) calls in a customer-oriented Call Center.
- **CTI (Computer-Telephony Integration):** Combining data with voice systems in order to enhance telephone services. For example, automatic number identification (ANI) allows a caller's records to be retrieved from the database while the call is routed to the appropriate party in a Call-Center.
- **Currency:** The point in time when updates were done. (e.g. the end of the prior day)
- **Custodian:** An individual who is responsible for the safekeeping, distribution, and/or disposal of (specific) I/T assets; authority is granted to the custodian by the asset Owner.
- **Data:** Groupings of related data elements that represent logical views of the data of business entities (e.g.: customers, policies, or providers).
- **Data Administration: Refers** to the management of data within the enterprise.
- **Data Base Administration: Refers** to the management of databases within the enterprise.
- **Database:** Structured or organized collection of information, which may be accessed by the computer; usually accessed through a DBMS.
- **Database Management System (DBMS): Computer** application program that accesses or manipulates the database; commercial examples include Sybase, Oracle, and Universal Database (UDB).

  DAP (Directory Access Protocol): The protocol which specifies how a client queries and receives responses from one or more servers in the a server's X.500 Directory Service. See LDAP.

- **Data Integrity:**

  (1) The state that exists when computerized data is the same as that in the source documents and has not been exposed to accidental or malicious alteration or destruction.

  (2) The property that data has not been exposed to accidental or malicious alteration or destruction.

- **DBMS (Database Management System): A** collection of programs that enables an application to create, read, update and delete information in a database.

- **Database:** A collection of information organized in such a way that a computer program can quickly select desired pieces of data. See DBMS.
- **Data Dictionary:** A specialized type of database containing metadata, which is managed by a data dictionary system; a repository of information describing the characteristics of data used to design, monitor, document, protect, and control data in information systems and databases; an application of data dictionary systems.
- **Data Element:** A basic unit of information having a meaning and that may have subcategories (data items) of distinct units and values.
- **Datagram:** In an IP network, a datagram is a unit of transmission (or packet) which contains the both the destination address and data.
- **Data, Meat:** See Metadata
- **Data Mart: A** subset of data from the information warehouse that has been massaged (e.g. summarized) to meet the needs of an individual or small group of knowledge workers.
- **Data Mining:** Exploration of large amounts of data, looking for previously unknown data patterns, analysis of known facts and discovery of unknown facts.
- **Data Replication: Reliable** delivery of large volumes of data updates from the source database to the target database (likely remote), which may have a different format. Data may be in the form of a snapshot, new data, or changes accumulated since the last update.
- **DBMS:** See Database Management System
- **DCE (Distributed Computing Environment)**: A suite of technology services developed by The Open Group for creating distributed applications that run on different platforms.
- **Digital Certificate An** attachment to an electronic message used for security purposes. The most common use of a digital certificate is to verify that a user sending a message is who he or she claims to be, and to provide the receiver with the means to encode a reply.

  An individual wishing to send an encrypted message applies for a digital certificate from a Certificate Authority (CA). The CA issues an encrypted digital certificate containing the applicant's public key and a variety of other identification information. The CA makes its own public key readily available.

  The recipient of an encrypted message uses the CA's public key to decode the digital certificate attached to the message, verifies it as issued by the CA and then obtains the sender's public key and identification information held within the certificate. With this information, the recipient can send an encrypted reply.

  The most widely used standard for digital certificates is X.509.

- **Domain Name:** A name that represents one or more IP addresses. Domain names are used in URLs to identify particular Web pages. When a Domain Name is specified, it must be translated through a DNS into a numeric IP address. For example, the domain name www.mbs.gov.on.ca might translate to 198.105.235.5.

  Every domain name has a suffix that indicates which Top Level Domain (TLD) it belongs to; in the URL http://www.mbs.gov.on.ca, the TLD is ca.

- **Domain:** A distinct functional area that can be supported by a family of systems with similar requirements and capabilities. An area of common operational and functional requirements.

- **Dynamic Load Balancing:** The ability to automatically involve more that one server for processing transactions.

- **De Facto Standards:** Components, products and technologies which have become generally accepted (e.g. through high market share) as 'standard'.

- **De Jure Standards:** Standards defined by organizations. Literally, "Standards by rule".

- **DES (Data Encryption Standard): A** secret key cryptography method that uses a 56-bit key. DES is based on an IBM algorithm which was further developed by the U.S. National Security Agency. DES decryption is very fast and widely used. The secret key may be kept a total secret and used over again. Or, a key can be randomly generated for each session, in which case the new key is transmitted to the recipient using a public key cryptography method.

  Triple DES is an enhancement to DES that provides considerably more security than standard DES, which uses only one 56-bit key. There are several Triple DES methods. EEE3 uses 3 keys and encrypts 3 times. EDE3 uses 3 keys to encrypt, decrypt and encrypt again. EEE2 and EDE2 are similar to EEE3 and EDE3, except that only 2 keys are used, and the first and third operations use the same key.

- **Distributed When** used to modify terms like system, objects, application, refers to such items that form a co-operating collection spanning several processors.

- **DMZ (DeMilitarized Zone):** A Demilitarized Zone is used by an enterprise to separate, for security reasons, the “outside’ environment from its internal network. The DMZ contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, and DNS servers. Firewalls are used define and secure the internal and external boundaries of the DMZ.

- **DNS (Domain Name Service):** An Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.example.com might translate to 198.105.232.4.

  If one DNS server doesn't know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

- **EDI (Electronic Data Interchange):** EDI involves the electronic exchange of data among transmission among business partners in a standard format. Billings and purchases are examples of types of EDI data which is interchanged electronically.
- **Electronic Mail (e-mail):** Communication, processed through a network, from one workstation to another. E-mail, is an end-user application for person-to-person messaging (from one person's out-basket to another person's in-basket).
- **Electronic Signatures:** Used to establish accountability and authenticity of electronic transactions through the use of public and private keys.
- **Encryption:** A method of providing data security when stored on disk or transmitted over networks. Because encryption/decryption techniques are powerful, the U.S. government regulates their export outside of the U.S. and Canada.
- **Enterprise:** The highest level in an organization - includes all missions and functions. Typically, a large commercial or government organization, or a subset of one. Enterprises pose particular challenges to the designers of IT Solutions. In particular, scalability, integrity, performance and access to legacy systems are fundamentally important.
- **Enterprise Model:** A high-level model of an organization's mission, function, and information architecture. The model consists of a function model and a data model.
- **Entity:** Generically, something that has separate and distinct existence and objective or conceptual reality.
- **Evaluation Criteria:** Guidelines for comparing or judging the appropriate use of information technology in the business.
- **Firewall:** When an enterprise is connected to the Internet, firewalls are used to secure the enterprise's internal network (and its information assets) from internet Users. Under current best practices, the enterprise is isolated from the outside world by a DMZ, and both the internal and external facing boundaries of the DMZ are protected by firewalls.
- **FTP (File Transfer Protocol):** The protocol used on the Internet for sending files.
- **Gateway:** A special purpose, dedicated computer that attaches to two or more networks and routes packets from one to the other. The term is loosely applied to any machine that transfers information from one network to another, as in mail gateway.
- **Granularity:** The level of detail contained in a unit of data. Data with a high level of detail has a low level of granularity.
- **Graphical User Interface (GUI):** A Human-Computer Interface design that allows the user to effect commands, enter into transaction sequences, and receive displayed information through graphical representations of objects (menus, screens, buttons, etc.). Contrast with Green-screen interface.

- **Green-Screen Interface:** A non-bit mapped character-based human-computer interface in which the primary form of interaction between the user and system is through text. Contrast with Graphical User Interface.
- **Guidelines:** Guidelines are recommendations related to the use of products or technologies; they are not standards, and compliance to guidelines is not mandatory.
- **GUI:** See Graphical User Interface.
- **Home Page: The** main page of a Web site. Typically, the home page serves as an index or table of contents to other documents stored at the site.
- **HTML (HyperText Markup Language):** The authoring language used to create documents on the World Wide Web.
- **HTTP (HyperText Transfer Protocol):** The underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page.

  The other main standard that controls how the World Wide Web works is HTML, which covers how Web pages are formatted and displayed.

  HTTP is called a stateless protocol because each command is executed independently, without any knowledge of the commands that came before it.
- **IMAP** or **Internet Message Access Protocol: A** protocol for retrieving e-mail messages. The latest version, IMAP4, is similar to POP3 but supports some additional features.
- **Information Catalogue:** A repository for the storage and retrieval of metadata, typically used to support users in an informational environment.
- **Information:** Generically, data which reduces ambiguity More commonly, used to mean communication or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audio-visual forms
- **Information Domain:** A set of commonly and unambiguously labelled information objects with a common security policy that defines the protections to be afforded the objects by authorized users and information management systems.
- **Information Management (IM):** The creation, use, sharing, and disposition of information as a resource critical to the effective and efficient operation of functional activities. The structuring of functional processes to produce and control the use of data and information within functional activities, information systems, and computing and communications infrastructures.
- **Information Resources Management (IRM):** The planning, budgeting, organizing, directing, training, promoting, controlling, and management activities associated with

the burden (cost), collection, creation, use, and dissemination of information by Agencies and includes the management of information and related resources.

- **Information Systems (IS):** Computer hardware, computer software, telecommunications, information technology, personnel, and other resources that collect, record, process, store, communicate, retrieve, and display information. An IS can include computer software only, computer hardware only, or a combination of the above.
- **Information Technology (IT):**
    - the technology included in hardware and software used for processing information, or
    - the organization responsible for information technology within a company.
- **Information Technology Architecture (ITA):** A series of principles, standards, guidelines or business rules used by an organization to direct the process of planning, acquiring, building, retiring and/or modifying technology components and resources throughout the enterprise. These resources can include but are not limited to hardware, software, models, procedures, and people.
- **Infrastructure:** Infrastructure includes platforms, services and communications (i.e. is anything outside of the domain of applications). Collectively, infrastructure must meet the performance requirements of and capacity for data and application requirements.
- **Interoperability:**
    - The ability of two or more systems or components to exchange data and use information;
    - The ability of two or more systems to exchange information and to mutually use the information that has been exchanged.
- **Intranet:** The technology platform to support access to internal information and business applications using web-based technologies, in particular the HTTP protocol and Web servers and browsers.
- **Integration:** The result of an effort that joins two or more similar products such as individual system elements, components, modules, processes, databases, or other entities, and produces a new product that functions, as a replacement for the two or more similar but less capable entities (products), in a framework or architecture in a seamless manner.
- **Interface:** Interconnection and interrelationships between two devices, two applications, or the user and an application or device.
- **Internet:** A worldwide association of TCP/IP-based interconnected networks. Within a private network, IP addresses can be assigned at random as long as each one

is unique. However, if a private network is to be connected to the Internet, IP addresses must be registered to avoid duplicates.

- **Internet Backbone:** high-speed link spanning the world from one major metropolitan area to another, provided by a handful of Internet service providers (ISPs). These ISPs use connections running at approximately 45 mbps (T3 lines) linked up at specified interconnection points called Network Access Points (which are located in major metropolitan areas). Local ISPs connect to this backbone through routers so that data can be carried though the backbone to its destination.
  Internet Telephony: See Voice over IP.

- **Interoperability:** The ability of software and hardware on multiple machines from multiple vendors to communicate and share information meaningfully.

- **IP (Internet Protocol):** Specifies the format of packets, also called datagrams, and the addressing scheme. Most networks combine IP with a higher-level protocol called Transport Control Protocol (TCP), which establishes a virtual connection between a destination and a source.

  The current version of IP is IPv4. A new version, called IPv6, is under development.

- **IP Address:** An identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255. For example, 1.190.12.240 could be an IP address.

- **IPSec**, or **IPSecurity** A set of protocols designed to support secure exchange of packets at the IP layer. IPsec is expected to be deployed widely to implement Virtual Private Networks (VPNs).

  IPsec supports two encryption modes: Transport and Tunnel. Transport mode encrypts only the data portion (payload) of each packet, but leaves the header untouched. The more secure Tunnel mode encrypts both the header and the payload. On the receiving side, an IPSec-compliant device decrypts each packet.

  IPsec depends upon the sending and receiving devices sharing a public key. This is accomplished through a protocol known as Internet Security Association and Key Management Protocol/Oakley (ISAKMP/Oakley), which allows the receiver to obtain a public key and authenticate the sender using digital certificates.

- **ISP or Internet Service Provider:** A company that provides a direct connection from an enterprise's networks to the Internet. ISPs themselves are connected to one another through Network Access Points (NAPs).

- **IVR:** Interactive Voice Response system.

- **JAR (Java Archive Repository):** A file format used to bundle all components required by a Java applet. JAR files simplify the downloading of applets since all the components (class files, images, sounds, etc.) can be packaged into a single file. In

addition, JAR supports data compression, which further decreases download times. By convention, JAR files end with a .jar extension.

- **Java:** A high-level programming language developed by Sun Microsystems.

  Java is an object-oriented language similar to C^{++}, but simplified to eliminate language features that cause common

  programming errors. Java source code files (files with a .Java extension) are compiled into a format called bytecode (files with a .class extension), which can then be executed by a Java interpreter. Compiled Java code can run on most computers because Java interpreters and runtime environments, known as Java Virtual Machines (VMs),

  exist for most operating systems, including UNIX, the Macintosh OS, and Windows. Bytecode can also be converted directly into machine language instructions by a just-in-time compiler (JIT).

  Java is a general purpose programming language with a number of features that make the language well suited for use on the World Wide Web. Small Java applications are called Java applets and can be downloaded from a Web Server and run on a client by a Java-compatible Web browser, such as Netscape Navigator or Microsoft Internet Explorer.

- **JavaBeans:** A component model for Java that lets developers create reusable software objects.

- **JavaScript** A scripting language developed by Netscape to enable Web authors to design interactive sites. Although it shares many of the features and structures of the full Java language, it was developed independently. JavaScript can interact with HTML source code, enabling Web authors to spice up their sites with dynamic content. JavaScript is open language that anyone can use without purchasing a license. It is supported by recent browsers from Netscape and Microsoft, although Internet Explorer supports only a subset, which Microsoft calls Jscript.

- **JVM (Java Virtual Machine):** A JVM acts as an interpreter between and a computer's operating system and the Java bytecode. JVMs enable the portability of Java applets, since that the same Java code can be run in a JVM on platforms for which JVMs have been implemented, including Macintosh, Windows, and Unix. JVMs read and execute (interpret) Java statements one at a time so they are often slower than a just-in-time compiler.

- **JIT (Just In Time Compiler): When** dealing with Java, a just-in-time compiler converts Java bytecode (compiled Java source language statements) into native code designed to run on a specific hardware and operating system platform. Since it compiles all the code at once before execution, Java programs often run faster with a JIT than with a Java Virtual Machine.

- **LAN:** See Local Area Network.

- **Leased Line:** A dedicated telecommunications point to point line.

- **LDAP (Lightweight Directory Access Protocol):** A set of protocols for accessing information directories. LDAP is based on the standards contained within the X.500 standard, but is significantly simpler than DAP. Unlike X.500, LDAP supports TCP/IP, which is necessary for any type of Internet access. Because it's a simpler version of X.500, LDAP is sometimes called X.500-lite.

  Although not yet widely implemented, LDAP should eventually make it possible for almost any application running on virtually any computer platform to obtain directory information, such as email addresses and public keys. Because LDAP is an open protocol, applications need not worry about the type of server hosting the directory.

- **Legacy Systems:** Systems that are candidates for phase-out, upgrade, or replacement.

- **Life Cycle:** The period of time that begins when a system is conceived and ends when the system is no longer available for use. It generally refers to the usable system life.

- **Local Area Network:** The interconnection of several personal computers and other hardware such as printers. Designed originally as a means of sharing hardware and software amongst PCs; now used as a general means of communication between PCs.

- **Logical** Node**:** A logical aggregation of IT components and/or services. Logical nodes are product and vendor independent system "building blocks" which are defined in terms of the function they provide.

  When designing a system, a designer initially specifies the logical nodes needed to meet the system's functional requirements; as the design progresses, the components and services are mapped to real technologies and products, and the logical nodes are mapped to physical nodes.

- **Market Acceptance:** Accepted in the market as evidenced by annual sales, length of time available for sale, availability of skills and after-sale (including third-party) support.

- **Middleware:** The term middleware is used to describe separate products, generally invoked by an API, that serve as the glue between multiple applications or tiers. Common middleware categories include:

  - TP monitors
  - DCE environments
  - RPC systems
  - Object Request Brokers (ORBs)
  - Database access systems (see DBMS)
  - Message Queuing or Message Passing

- **MAPI:** Messaging Application Programming Interface.

- **Metadata:** Data about data - the description of the structure, content, keys, indexes, etc. of data.
- **MIME:** Multipart Internet Mail Extension.
- **Messaging and Queuing:** Message queuing (MQ) is a technique used to communicate from program to program. It can be used within any application where programs need to communicate with each other. MQ communication is performed by the programs sending messages to each other using queues. The messages contain application data that is passed from one part of the application to another. The parts of the application can be on the same system or on separate systems in a network.
- **Mobile Computing:** The ability to use or generate computer-based information anytime and anywhere, without being tied to a specific physical location. The most common form of mobile computing is communications with a server system from notebook and laptop computers.
- **Multimedia:** The integrated presentation of text, graphics, video, animation, and sound.
- **NAP (Network Access Point)** a public network exchange facility where Internet Service Providers (ISPs) can connect with one another in peering arrangements. The NAPs are a key component of the Internet backbone because the connections within them determine how traffic is routed. They are also the points of most Internet congestion.
- **NAT (Network Address Translation)**: An Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. A NAT box located where the LAN meets the Internet makes all necessary IP address translations.

  NAT serves the following purposes:

  - Provides a type of firewall by hiding internal IP addresses
  - Enables a company to use more internal IP addresses. Since they're used internally only, there's no possibility of conflict with IP addresses used by other companies and organizations.
- **Network:** The connecting of computing devices via hardware and software.
- **Node:** Location in a computer network. A node may be a logical or physical client or server.
- **Non-repudiation:** The ability to verify the originator of a message, typically through the use of electronic signatures.
- **Non-trusted Systems:** Connected systems from which a requester for service cannot be authenticated.

- **Object-Oriented Programming:** A type of programming in which programmers define not only the data type of a data structure, but also the types of operations (functions) that can be applied to the data structure. In this way, the data structure becomes an object that includes both data and functions. In addition, programmers can create relationships between one object and another; for example, objects can inherit characteristics from other objects.

- **Open System:** A system that implements sufficient open specifications for interfaces, services, and supporting formats to enable properly engineered components to be utilized across a wide range of systems with minimal changes, to interoperate with other components on local and remote systems, and to interact with users in a style that facilitates portability.

  To be considered open, a system must have all of the following characteristics:

  (1) Use well defined, widely used, non-proprietary interfaces/protocols

  (2) Use of standards which are developed/adopted by industrially recognized standards bodies

  (3) Definition of all aspects of system interfaces to facilitate new or additional systems capabilities for a wide range of applications

  (4) Explicit provision for expansion or upgrading through the incorporation of additional or higher performance elements with minimal impact on the system.

- **Operations Management:** A ***Systems Management discipline*** which supports the tasks associated with the planning, distributing, evaluating, and controlling the workloads and IT resources necessary to support those workloads. This includes: Resource Backup / Recovery, Control / Display, Automation, and Scheduling.

- **Owner:** an individual who is responsible and accountable to the enterprise for the acquisition, creation, use, safekeeping and disposal of (specific) information assets, which may include hardware, software, and/or data. Owners may delegate authority to Custodians in order to manage information assets on a day-to-day basis, but remain accountable to the Enterprise for activities performed on their behalf.

- **Patterns, Architectural:** See Templates, Architectural.

- **Page:** See Web Page.

- **Pattern:** "One thing expert designers know not to do is to solve every problem from first principles. Rather, they reuse solutions that have worked for them in the past. When they find a good solution, they use it over and over again. Such experience is part of what makes them experts. [Patterns] solve specific design problems and make [designs] more flexible, elegant and ultimately reusable. They help designers reuse successful designs by basing new designs on prior experience. A designer who is familiar with such patterns can apply them immediately to design

problems without having to rediscover them" [Gamma 95]. See Architectural Templates.

- **PBX (Private Branch Exchange):** The private telephone network used within an enterprise. Users of the PBX share a certain number of outside lines for making telephone calls external to the PBX.

  Most medium-sized and larger companies use a PBX because it's much less expensive than connecting an external telephone line to every telephone in the organization. In addition, it's easier to call someone within a PBX because the number Users need to dial is typically just 3 to 5 digits.

  Some organizations use a Centrex system , which is a PBX with all switching occurring at a local telephone office instead of at the company's premises.

- **Performance Management:** A *Systems Management discipline* which provides tools and procedures required to monitor usage of the system resources and provide proactive resource management (including capacity planning).

- **Physical Network:** The physical network includes the actual hardware that supports the network including all items in the LAN, WAN, wireless, and personal area network, including wires, routes, hubs, bridges, switches, adapter cards, controllers, fiber, wiring closet patch panels, transmitters, receivers, etc

- **Platform:** The application platform is defined as the set of resources that support the services on which application software will execute.

- **PIN Numbers:** Personal Identification Numbers.

- **Portability:** The ease with which a system, component, data, or user can be transferred from one hardware or software environment to another.

- **Private Key:** A key known only to the recipient of a message, which can be used to decrypt messages encrypted with the recipient's public key.

- **PSTN (Public Switched Telephone Network):** Refers to the international telephone system based on copper wires carrying analog voice data. This is in contrast to leased (i.e.non-public) networks, and to newer telephone networks base on digital technologies.

- **Policy:** High level, official statements that guide how information technology is to be used or managed within the organization.

- **POP (Post Office Protocol):** A protocol used to retrieve e-mail from a mail server. Most e-mail clients use the POP protocol, although some can use the newer IMAP (Internet Message Access Protocol).

  There are two versions of POP. The first, called POP2, became a standard in the mid-80's and requires SMTP to send messages. The newer version, POP3, can be used with or without SMTP.

- **Proprietary:** Privately owned and controlled by a vendor

- **Problem Management:** A ***Systems Management discipline*** which supports the tasks for managing problems and incidents from their detection through final resolution. This includes Problem Detection, Problem Tracking, Problem Resolution, and Problem Recovery.

- **Process Model:** Provides a framework for identifying, defining, and organizing the functional strategies, functional rules, and processes needed to manage and support the way an organization does or wants to do.

- **Protocol:** An agreed-upon format for transmitting data between two devices. A protocol is the set of conventions that a receiver and sender use to ensure that the message can be received and processed by the receiver.

  Because of the complex requirements of protocols, complex protocols, which are designed for specific purposes (e.g. file transfer, terminal emulation, electronic mail, etc) are normally layered 'on-top' of other protocols, in what is commonly referred to a 'protocol stack'.

- **Proxy Server** A server that sits between a client application, such as a Web browser, and a real server. Proxy servers are available for common Internet services; for example, an HTTP proxy is used for Web access, and an SMTP proxy is used for e-mail. Proxies generally employ network address translation (NAT), which presents one organization-wide IP address to the Internet. It funnels all user requests to the Internet and fans responses back out to the appropriate users. Proxies may also cache Web pages, so that the next request can be obtained locally.

- **Public Key Encryption:** An asymmetric cryptographic system that uses two keys -- a public key known to everyone and a private or secret key known only to the recipient of the message. When A wants to send a secure message to B, he uses B's public key to encrypt the message. B then uses his or her private key to decrypt it.

  In the public key system, the public and private keys are related in such a way that only the public key can be used to encrypt messages, and only the corresponding private key can be used to decrypt them. Moreover, it is virtually impossible to deduce the private key if you know the public key.

- **Query Tool:** A business support tool that allows the user to interact directly with a DBMS to retrieve and format data.

- **RDBMS (Relational Database Management System):** A database system, or DBMS, in which data is organized into tables. Data in each table is maintained in rows; the rows contain one or more columns. The data in a row and column in one table can be defined to maintain one or more relationships with data in other tables.

- **Referential Integrity:** The facility of a DBMS to ensure the validity of predefined relationships.

- **Reporting Tool:** A robust tool for developing canned or scheduled reports or queries..

- **Repository:** A common place for the storage of a variety of objects (e.g. data models, metadata, and source code).
- **Router:** A device that forwards data packets from one local area network (LAN) or wide area network (WAN) to another. Based on routing tables and routing protocols, routers read the network address in each transmitted frame and make a decision on how to send it based on the most expedient route (traffic load, line costs, speed, bad lines, etc.).

  Routers are used to segment LANs in order to balance traffic within workgroups and to filter traffic for security purposes and policy management. Routers are also used at the edge of the network to connect remote offices. Multiprotocol routers support several protocols such as IP, IPX, AppleTalk and DECnet.

  Routers can only route a message that is transmitted by a routable protocol such as IP or IPX. Messages in non-routable protocols, such as NetBIOS and LAT, cannot be routed, but they can be transferred from LAN to LAN via a bridge. Because routers have to inspect the network address in the protocol, they do more processing and add more overhead than a bridge or switch.
- **RPC (Remote Procedure Call):** One of three means of communication. Issuing an RPC is analogous to calling a subroutine, except that the subroutine may exist somewhere else within the network. Alternatives to RPCs include messaging, and the conversational model of communications.
- **Scalability:** The ability to easily move components of an application from one computing platform to another as the needs of the system grow or shrink.
- **Scanned Signatures:** Digitally imaged signatures.
- **Scenario:** A description of a potential execution trace e.g. transactional access by customers and suppliers via the Web.
- **Socks:** A protocol for handling TCP traffic through a proxy server. It can be used with virtually any TCP application, including Web browsers and FTP clients. It enables a simple firewall mechanism because it checks incoming and outgoing packets and hides the IP addresses of client applications. There are two main versions of SOCKS -- V4 and V5. V5 adds an authentication mechanism for additional security.
- **Stovepipe System:** A system, often dedicated or proprietary, that operates independently of other systems. The stovepipe system often has unique, nonstandard characteristics.
- **Security:**

  (1) The combination of confidentiality, integrity, and availability, or

  (2) The quality or state of being protected from uncontrolled losses or effects.

Note: Absolute security may in practice be impossible to reach; thus the security "quality" is relative. Within state models of security systems, security is a specific "state" that is to be preserved under various operations.

- **Security Management:** A ***Systems Management discipline*** which manages the security of IT assets including the physical security of equipment, software, and data, and the registration of users and their access to IT services
- **Server:** As in client/server computing, the node which responds to requests from the client.
- **S-HTTP:** An extension to the HTTP protocol to support sending data securely over the World Wide Web. Not all Web browsers and servers support S-HTTP.

  Secure Sockets Layer (SSL) is another technology for transmitting secure communications over the World Wide Web which is more prevalent than S-HTTP. The two protocols have very different designs and goals so it is possible to use them together. SSL is designed to establish a secure connection between two computers, S-HTTP is designed to send individual messages securely.
- **SMTP (Simple Mail Transfer Protocol):** A widely used E-mail protocol developed by Internet. Extremely popular in the USA; less popular in Europe, where X.400 is preferred.
- **SNMP** or **Simple Network Management Protocol:** A network management protocol used in TCP/IP Local Area Networks.
- **SSL (Secured Sockets Layer):** Secure Sockets Layer is a protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a private key to encrypt data that's transferred over the SSL connection. Both Netscape Navigator and Internet Explorer support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, Web pages that require an SSL connection start with https: instead of http.

  When an SSL session is started, the browser sends its public key to the server so that the server can securely send a secret key to the browser. The browser and server exchange encrypted data during that session. SSL has been merged with other protocols and authentication methods into a new protocol known as Transport Layer Security (TLS).

  Another protocol for transmitting data securely over the World Wide Web is Secure HTTP (S-HTTP). Whereas SSL creates a secure connection between a client and a server, over which any amount of data can be sent securely,

  S-HTTP is designed to transmit individual messages securely. SSL and S-HTTP, therefore, can be seen as complementary rather than competing technologies. Both protocols are international standards.
- **Stakeholders:** Any individuals or groups which have a vested interest (in an architecture, system, or application).

- **Standards based architecture:** An architecture based on an acceptable set of standards governing the arrangement, interaction, and interdependence of the parts or elements that together may be used to form systems, and whose purpose is to insure that a conformant system satisfies a specified set of requirements.
- **System:**
  (1) People, machines and methods organized to accomplish a set of specific functions.
  (2) An integrated composite of people, products, and processes that provides a capability or satisfy a stated need or objective
  (3) those items that produce, use or exchange information.
- **Response Time:** The ability to react to requests within established time criteria. To be operationally effective, the system must product the desired output in a timely manner based on system category for routine or priority operations.
- **Scalability:**
  (1) The ability to use the same application software within a range of hardware/software platforms from personal computers to super computers.
  (2) The capability to grow to accommodate increased workloads (e.g. number of users, transaction volumes, quantity of data).
- **Single Logon:** Allows User to have a single identification within the network, log on with a single password, and have access to all the network facilities for which they are authorized.
- **SMTP (Simple Mail Transfer Protocol):** The TCP/IP standard protocol for sending e-mail messages between servers. Most e-mail systems that send mail over the Internet use SMTP to send messages from one server to another; the messages can then be retrieved with an e-mail client using either POP or IMAP.
- **SOCKS Server:** (SOCKetS server) A proxy server that functions as a general-purpose TCP/IP proxy and handles any kind of traffic (HTTP, SMTP, FTP, Telnet, etc.). Major Web browsers support SOCKS.
- **Standards[1]:** A published document or convention that establishes uniform engineering and technical requirements for processes, procedures, practices, interfaces and/or methods. Standards may also establish requirements for selection, application, and design criteria.
- **Standards[2]:** Enterprise constraints over the specification, selection, and implementation of technologies or products. Unlike guidelines, compliance with standards is mandatory.
- **Symmetric Encryption:** A type of encryption where the same key is used to encrypt and decrypt the message. This differs from asymmetric encryption, which uses one

key to encrypt a message and another to decrypt the message. Public-key systems are asymmetric.

  - **Synchronous** An event that occurs at a time that is related to or dependent on the time at which another event occurs. The relationship between the time the events occur is predictable.

- **TCP (Transmission Control Protocol):** One of the main protocols in TCP/IP networks. Whereas the IP protocol deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

- **TCP/IP:** The suite of communications protocols used to connect hosts on the Internet. TCP/IP uses several protocols, the two main ones being TCP and IP. TCP/IP. TCP/IP is the de facto standard for transmitting data over the internet.

- **Templates, Architectural:** Templates are design patterns that can be applied generically to a specific domain. The ATFB Logical Enterprise Architecture, for example, provides templates (Logical Nodes and their relationships) for the Call Center, Asynchronous Collaboration, Workflow, and Internet domains. These templates are based on industry best practices.

- **Thin Client:** a client node with limited (or no) data or application functions – a PC running a browser is an example of a thin client – all data and function are stored on servers, and the browser and PC provide only the User interface.

- **TLS (Transport Layer Security):** A security protocol that is a merger of SSL and other protocols. It is expected to become a major security standard on the Internet, eventually superseding SSL. TLS is backward compatible with SSL and uses Triple DES encryption.

- **Top Level Domain (TLD):** Part of a domain name. Every domain has a suffix that indicates which top-level (TLD) domain it belongs to. There are only a limited number of such domains. Examples include .gov (Government agencies), .edu (Educational Institutions), .org (Non- profit Organizations), .mil (Military), .com (Commercial business), .net (Network organizations), and .ca (Canada) .

- **Trusted Systems:** A system or group of systems configured in a fully secured and controlled environment. i.e. all users and access points are known and pre authorized.

- **Unix:** An operating system originally designed by AT&T and enhanced by the University of California at Berkeley and others. Since it was powerful and essentially free, it became very popular at universities. Many vendors made their own versions of Unix available.

- **URL (Uniform Resource Locator):** The global address of documents and other resources on the World Wide Web. The first part of the address indicates what protocol to use, and the second part specifies the IP address or the Domain Name where the resource is located. When a Domain Name is specified, it must be

translated through a DNS into a numeric IP addresses. For example, the domain name www.example.com might translate to 198.105.232.4.

- **User:** Any person, organization, or functional unit that uses the services of an information processing system
- **VOIP (Voice over IP):** The transmission of voice signals (e.g. telephone) over an IP network. When the public Internet is the transport vehicle, it is referred to as "Internet telephony."

  Private networks can provide from good to excellent quality, matching that of the PSTN. Over the Internet, voice quality varies considerably; however, protocols that support quality of service (dos) are expected to improve this condition. Nevertheless, Internet telephony means free voice calls as long as sending and receiving users have identical software that uses proprietary techniques or compatible software that uses the H.323 standard
- **VPN (Virtual Private Network):** A network that is constructed by using public wires to connect nodes. For example, there are a number of systems that enable you to create networks *using the Internet* as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.
- **WAN:** A Wide Area Network (WAN) is a network that provides communications services to a geographic area larger than that served by a local area network and that may use public communications facilities from regulated carriers outside of the enterprise. Standards include HDLC, SDLC, X.25, ISDN, and Frame Relay.
- **Web (World Wide Web)** The network of Internet servers that support specially formatted documents in a language called HTML. The documents are viewed through a browser, and support links to other documents, as well as graphics, audio, and video files.
- **Web Browser:** See Browser**.**
- **Web Page:** A document on the World Wide Web. Every Web page is identified by a unique URL (Uniform Resource Locator).
- **Web Site:** A site (location) on the World Wide Web. Each Web site contains a home page, which is the first document users see when they enter the site. The site might also contain additional documents and files. Each site is owned and managed by an individual, company or organization.
- **Workflow:** The completion of a task or tasks through the directed movement of information from an initial state to a final state; state changes may or may not involve multiple participants.
- **Workflow Manager** Manages the flow and assignment of work within and between different communities via queues associated with an assignable entity (e.g., a person, a department, an IT service such as automated FAX delivery). A workflow manager

maintains the context of the work over an extended time and over multiple working sessions with possibly multiple assigned entities.

- **XML (eXtensible Markup Language):** A flexible way to create common information formats and share both the format and the data on the World Wide Web, intranets, and elsewhere.

  As an example, auto makers might agree on a standard or common way to describe the information about an automobile (Make, model, color, engine displacement, options, current location, retail price), and then describe the product information format with XML. Such a standard way of describing data would enable a broker or dealer to send an intelligent agent (a program) to the auto maker's Web site, gather data, and then make a selection or actually place an order

  XML can be used by any individual or group of individuals or companies that wants to share information in a consistent way.

- **X.400:** An international standard for addressing and transporting e-mail messages.

- **X.500** An international standard that defines how global directories should be structured. X.500 directories are hierarchical with different levels for each category of information, such as country, state, and city. X.500 supports X.400 systems.

  In the X.500 directory architecture, the client queries and receives responses from one or more servers in the server's Directory Service, with the Directory Access Protocol (DAP) controlling the communication between the client and the server.

  Since the X.500 Directory Access Protocol (DAP) is too complex for most directory implementations, the University of Michigan developed a simpler TCP/IP-based version of DAP, called the Lightweight Directory Access Protocol (LDAP), for use on the Internet.

Portal Prototype

As a tool to help achieve a common understanding of the benefits of a portal a demonstration prototype has been developed. This portal prototype illustrates an "e-friendly" experience between the State of Missouri and its citizens, business, and visitors. The prototype is intended to demonstrate the ability to provide essential information and services. It also is designed to encourage the citizens and businesses of Missouri to interact electronically with their government.

As seen below in Figure 16, Portal Home Page and Figure 17, Alternate Portal Home Page, two design versions were provided.

Figure 16, Portal Home Page

The State of Missouri portal identifies three unique affinity groups or communities. Living represents citizens of Missouri, Business represents business operating within Missouri, and tourism represents visitors to Missouri. Each of these groups can immediately navigate to an area that is designed for their specific interests and/or requirements.

Starting with the home page, and on all pages, note the Top Navigation Bar. Convenient buttons denote:

- *Log In/Register* would enable users to identify themselves. This would allow for personalization of information, services, and transactions to the individual's needs and authorization.

- *State Government* would provide specific information on government branches, departments, and offices, as well as elected officials and their role in government.

- *Site Map* would provide a convenient map (both graphical and textual) to assist you in finding your way around the entire Web site.

- *Contact Us* serves as a means for feedback and specific requests. It would provide information contact names, contact titles/departments, mailing addresses, and phone/fax numbers along with the appropriate e-mail link.

- *Show Me* would serve as The State of Missouri's Portal search tool.

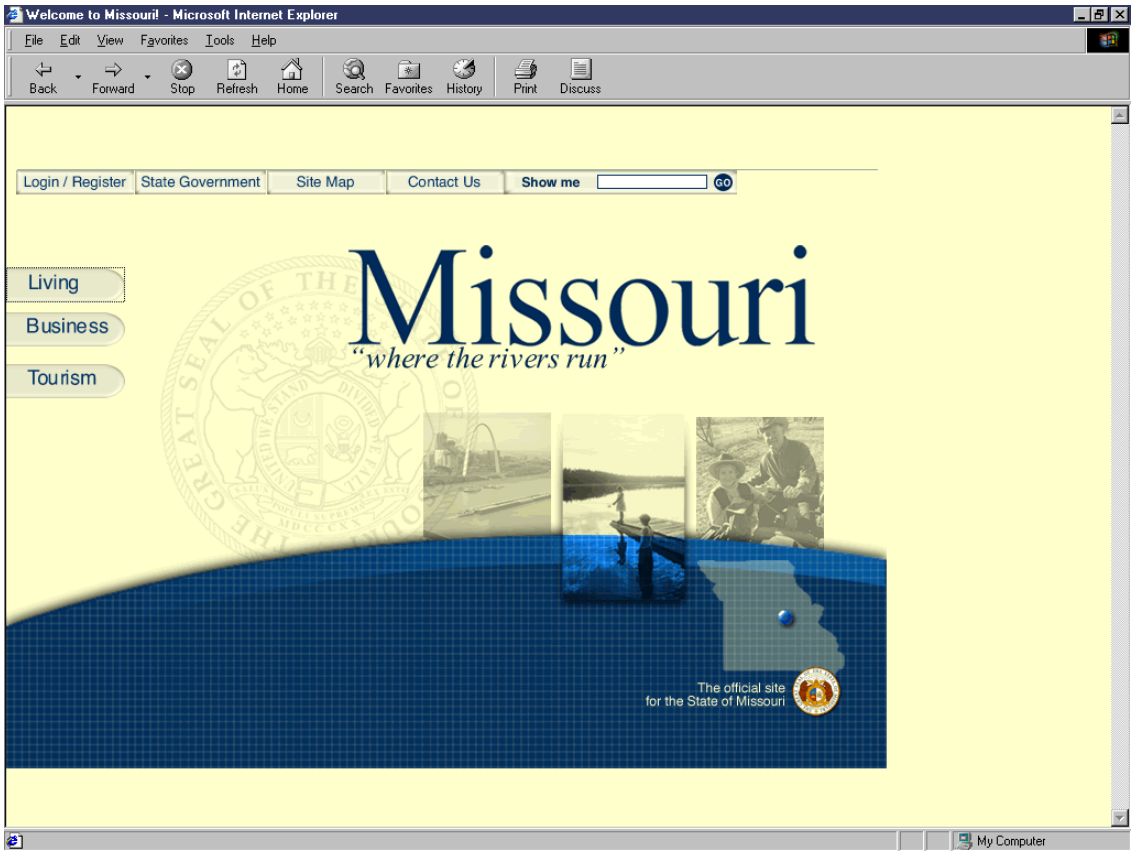


Figure 17, Alternate Portal Home Page

Select Living and you go to the Living page as shown in Figure 18. This provides access to such topical areas as: Student Tuition (MO$T), Communities, Schools, Recreation, Sports, Religion, Employment, and Community Connection.

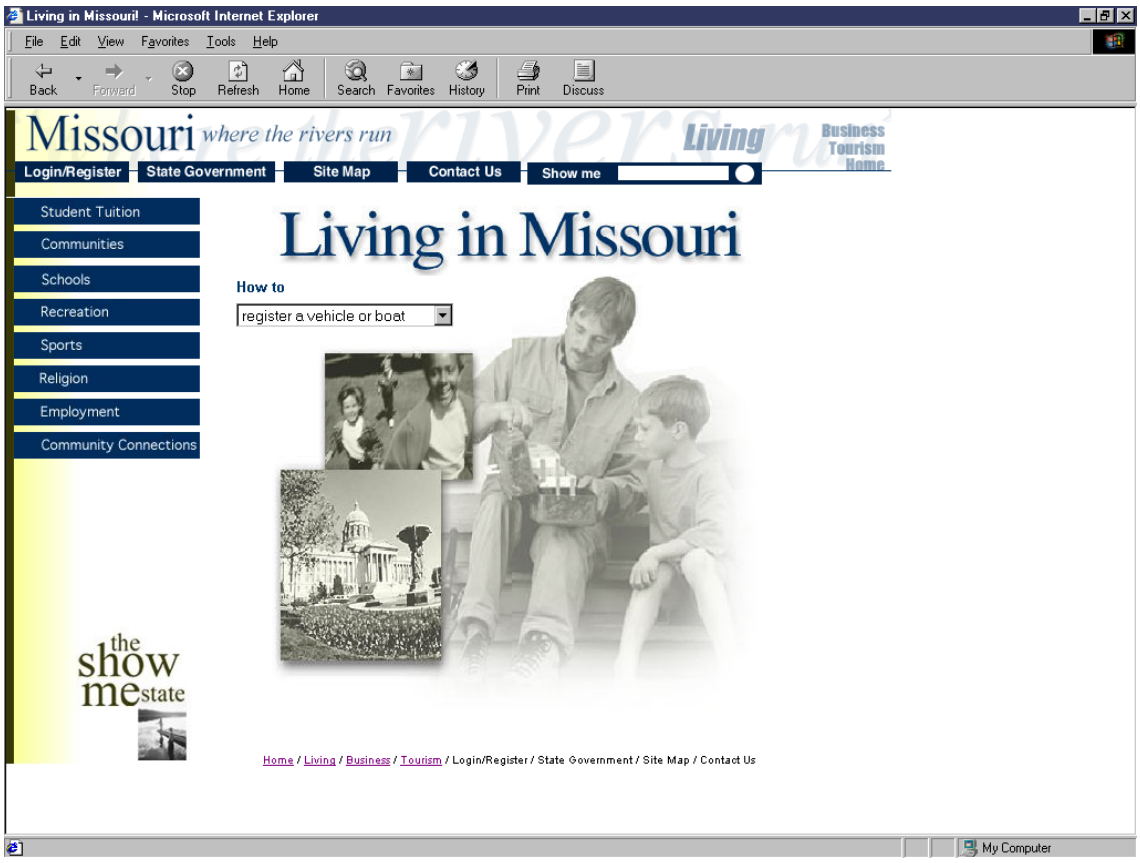


Figure 18, Portal Living Page

In the upper right hand corner of every page (with the exception of the homepage) there is a navigation tool that allows you to gain access to Living, Business, Tourism, and Home.

On each of the affinity group home pages there is a left navigation bar with listings of the important topics specific to that group.

Figure 19, the How to drop down box (which currently allow you to simply review the choices but not actually link to them) provides immediate access to appropriate transactions or information for the specific affinity group.

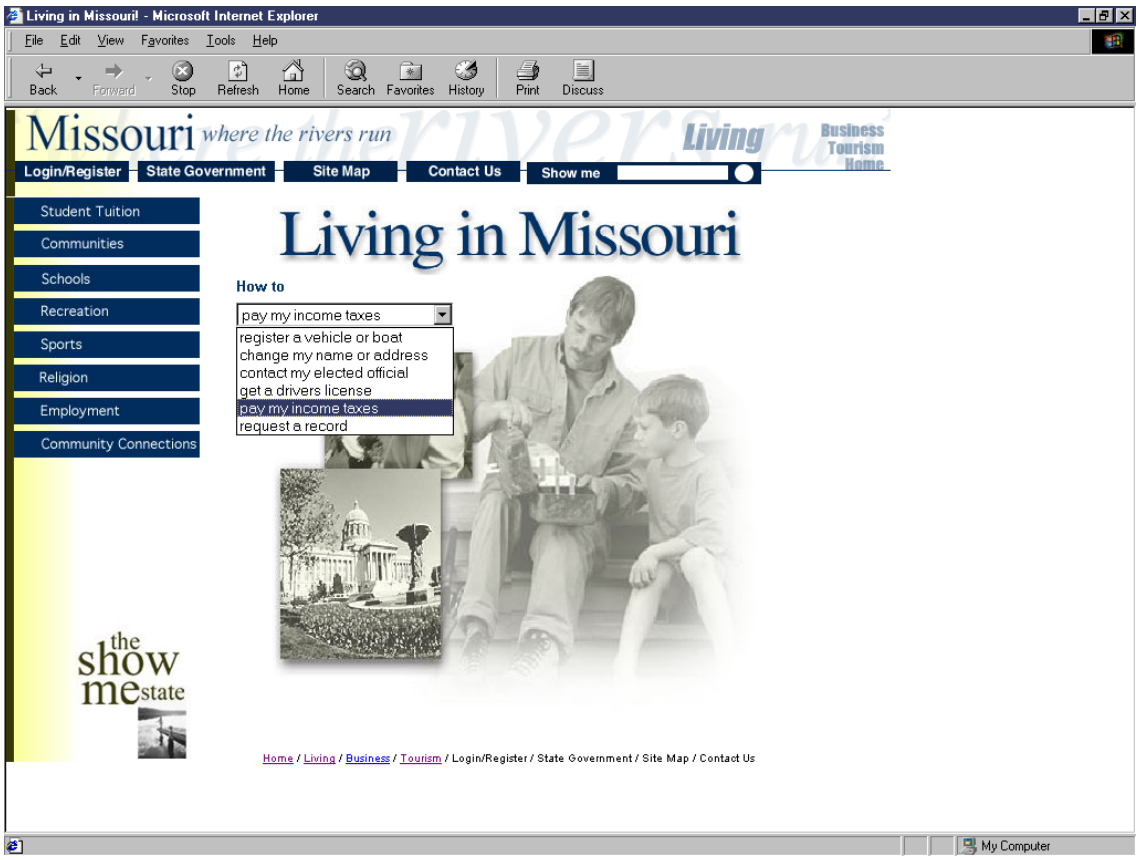


Figure 19, Living How To Section

For example, the Living How to section would include direct access to–register a vehicle or boat, change my name or address, contact my elected official, get a drivers license, pay my income taxes, and request a record, just to name a few.

Select Tourism and you go to the Tourism page shown in Figure 20, which provides such topics of interest as: Exploring Regions, Outdoor Adventures, Calendar of Events, Historic/Cultural, Where to stay.

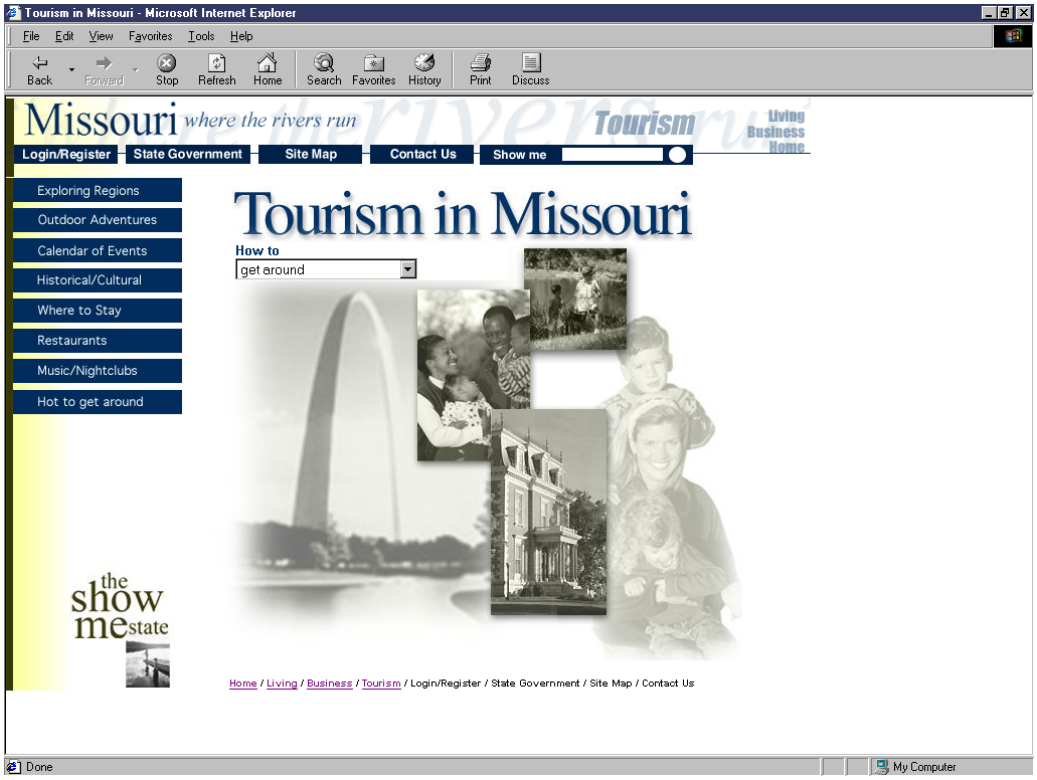


Figure 20, Tourism Page

Select Business and you go to the Business page as seen in Figure 21, The information and services available include: Doing business in Missouri, Starting a business, Regulations, Codes and Permits, Unemployment Insurance, Workers Comp, Organizations, and Employment.

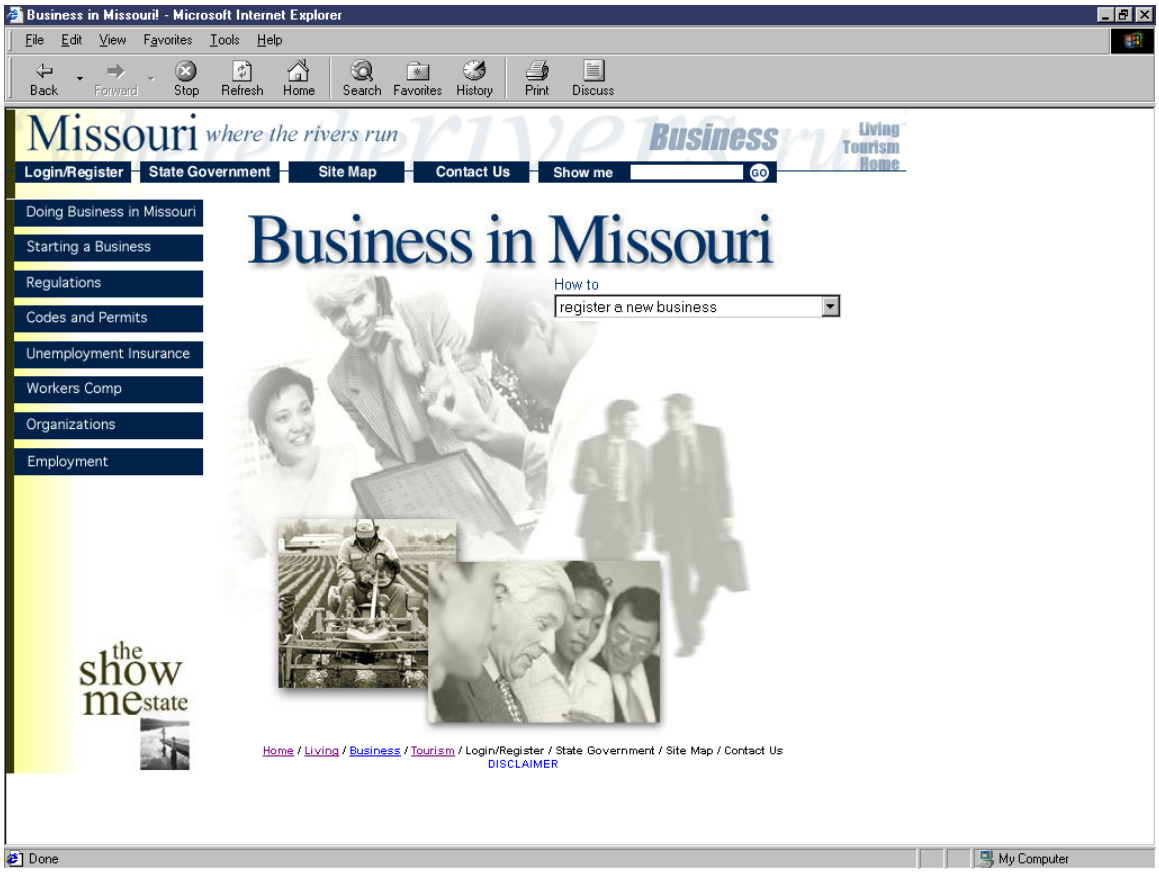


Figure 21, Business Page

Selecting Starting a Business provides a demonstration that takes you to an informational page shown in Figure 22. The page provides a special link that leads to a form to register a Limited Liability Company. This example, shown in Figure 23, illustrates the ease and simplicity of filling out and submitting forms online. The user completes the form and clicks submit on the finished page. Figure 24 illustrates a page that appears thanking the user and informing them that they will be contacted shortly.

Figure 22, Starting a business page

Figure 23, Articles of Organization

Figure 24, Acknowledgment

On the bottom of each page within the business section is a link that leads to a "flip - open" box that displays a Disclaimer of Liability issues pertinent to business and government.

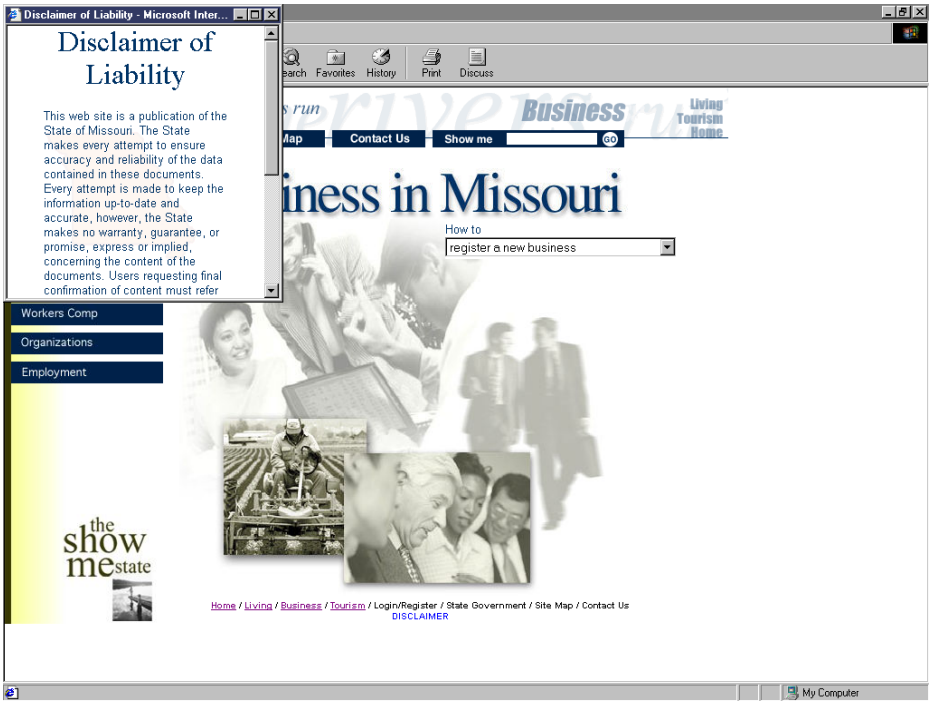


Figure 25, Disclaimer

Figure 26, Alternate Business Page

Figure 26 illustrates the alternate layout. Figure 27 shows the floating menu that appears when the Business option is selected. This depicts giving the user access directly to services that are on not associated with the current page.

Figure 27, Floating menu

Interviews

Interview Date/Time	Department	Senior Executive Interviewed	Additional Attendees
June 5	Office of the Governor	Mike Hartmann Deputy Chief of Staff	
June 1	Office of the State Treasurer	Bob Holden State Treasurer	Jill Hansen
June 1 .	Office of the Secretary of State	Rebecca Cook Secretary of State	Ron Welschmeyer
June 14	Office of the State Auditor	Claire McCaskill State Auditor	Max Joyce
June 1	Office of Administration	Richard Hanson Commissioner	Jim Schutt
June 1	Department of Agriculture	John Saunders Director	Robin Perso Sally Oxenhandler Gene Wiseman Lyndon Mote
June 5	Department of Conservation	Jerry Conley Director	David Erickson Jim Poole
June 9	Department of Corrections	Dora Schriro Director	Dave Schulte
June 5	Department of Economic Development	Joe Driskill Director	David Mitchem Don Lloyd
June 9	Department of Elementary & Secondary Education	Dr. Kent King Commissioner	Dr. Stephen Barr Betty Rottmann
June 14	Department of Health	Dr. Maureen Dempsey Director	Garland Land Rex Peterson
June 13 .	Department of Higher Education	Dr. Kala Stroup Commissioner	Dr. John Wittstruck Gina Hodge
June 8	Department of Insurance	Keith Wenzel Director	Marsha Mills Tim Dwyer
June 5	Department of Labor and Industrial Relations	Catherine Leapheart Director	Don Slinkard
June 13	Department of Mental Health	Patricia Graber Deputy Director	Gary Lyndaker
June 7	Department of Natural Resources	Jeff Staake Deputy Director	Chris Wilkerson
June 14	Department of Public Safety	Gary Kempker Director	
June 1	Department of	Quentin Wilson	Bill Perkins

	Revenue	Director	
June 5	Department of Social Services	Melba Price Associate Director	Dennis Bax
June 7	Department of Transportation	Henry Hungerbeeler Director	Pat Goff Lew Davison
June 5	Office of the State Courts Administrator	Judge William Price Chief Justice	Jim Roggero
June 8	MOSERS	Gary Findlay Director	
June 7	MO Ethics Commission	Charles Lamb Executive Director	Joseph Carroll Brian Hess
June 13	Public Defenders Office	Marty Robinson Director	Mary Willingham
June 7	MO Consolidated Health Care	Ron Meyer Executive Director	
June 13	MO Lottery	Jim Scroggins Director	Ron Murphy Mike Wankum

Documentation Provided

The State of Missouri provided the following documentation for review during this architecture assessment:

Hardcopy Document Name	Provided by	Document Date
Best Practices Summary (1 page)	Larry Seneker	5/2000
Treasurer's Office COTS summary	Larry Seneker	5/25/2000
Missouri Enterprise Architecture (draft)	Larry Seneker	1/31/2000
Department of Revenue Strategic Plan 1999-2002	Quentin Wilson	
Department of Revenue 5 year Web Plan	Bill Perkins	8/2/1999
Department of Agriculture Organization Chart	John Saunders	2/2/2000
Missouri Farm Facts - 1999	John Saunders	8/1999
Department of Agriculture Strategic Plan	John Saunders	
Missouri Blue Book	Rebecca Cook	3/31/2000
Dept. of Public Safety 1999 Annual Report	Gary Kempker	4/10/00
Veterans Commission / Survey info	Gary Kempker	6/5/00
Emergency Management / Survey info	Gary Kempker	6/6/00
Capitol Police / Survey info	Gary Kempker	6/6/00
Highway Safety / Survey info	Gary Kempker	6/6/00
Fire Safety / Survey info	Gary Kempker	6/6/00
Liquor Control / Survey info	Gary Kempker	6/6/00
Liquor Control / Strategic Plan	Gary Kempker	12/01/98
Liquor Control / Program Review	Gary Kempker	06/2000
Office of Administration organization chart	Dick Hansen	
Dept. of Insurance Annual Report	Keith Wenzel	1999
Department of Conservation Strategic Plan	Dave Erickson	3/21/00
Corrections Organizational Chart	Dora Shriro	3/24/2000
Mental Health "Lives Beyond Limitations"	Pat Graber	
Department of Corrections Integrated Strategic Plan 2001	Dora Schriro	11/23/1999
Department of Corrections Organizational Chart	Dora Schriro	3/24/2000
Correcting Corrections: Missouri's Parallel Universe	Dora Schriro	May 2000
Blueprint for Missouri Higher Education	Kala Stroup	6/2000
Division of Special Education org chart	Stephen Barr	
Stephen Barr's input - Special Education	Stephen Barr	
Marilou Joyner input – School Services	Marilou Joyner	
Office of the Missouri State Auditor 1999 Annual Report	Claire McCaskill	
Office of Administration Strategic Plan	Dick Hansen	7/1/99

Office of Administration Strategic Plan Results	Dick Hansen	

Softcopy Document Name	Provided by	Document Date
Elementary and Secondary Education Strategic Plan	**Betty Rottmann**	
Integrated Public Health Information Systems presentation	**Rex Peterson**	
Show Me Results		
IT Strategic Plan 2000	**Jan Grecian**	
ITPB Strategic Plan FINAL 1996	**Jan Grecian**	
OIT 1999 State of the State IT Report	**Jan Grecian**	
IT Strategic Plan Integration of New and Existing Objectives	**Jan Grecian**	
MISSOURI FEDERAL PRIORITIES FOR 2000		
SAMII Overview presentation		